

EXHIBIT 2

**IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

SECURITIES AND EXCHANGE)	
COMMISSION,)	
)	
Plaintiff,)	
)	Civil Action No. 1:23-cv-09518-PAE-BCM
v.)	
)	
SOLARWINDS CORP. and TIMOTHY G.)	
BROWN,)	
)	
Defendants.)	
)	

**EXPERT REPORT OF GREGORY RATTRAY
NOVEMBER 22, 2024**

TABLE OF CONTENTS

I.	Introduction	1
II.	Qualifications	2
III.	Instructions.....	5
IV.	Methodology	5
V.	The Representations In the Security Statement Accurately Describe SolarWinds’ Practices During the Relevant Period	7
A.	The Security Statement Merely Describes SolarWinds’ Basic Security Practices	8
B.	The Security Statement’s Representation About Following the NIST Framework Was Accurate.....	10
C.	The Security Statement’s Representations About Role-Based Access Controls Were Accurate.....	15
D.	The Security Statement’s Representations About Passwords Were Accurate	30
E.	The Security Statement’s Representations About Network Monitoring Were Accurate	38
F.	The Security Statement’s Representations About Software Development Were Accurate	45
VI.	The Graff Report is Fundamentally Flawed and Does Nothing to Change My Conclusions.....	54
A.	Mr. Graff Does Not Follow Any Valid Methodology	55
B.	Mr. Graff Misinterprets What It Means to Follow the NIST Framework	60
C.	Mr. Graff Does Not Show Any Systemic Failure to Implement Role-Based Access Controls	64
D.	Mr. Graff Does Not Show Any Systemic Failure to Implement Password Controls.....	86
E.	Mr. Graff Does Not Even Argue That SolarWinds Failed to Conduct Network Monitoring	97
F.	Mr. Graff Does Not Show Any Systemic Failure to Follow Secure Software Development Practices	98

I. INTRODUCTION

1. I have been retained on behalf of the Defendants in this matter to offer expert opinions regarding SolarWinds' cybersecurity program during the period October 19, 2018, to January 12, 2021, and in particular whether the program was consistent with certain representations in the Security Statement found on SolarWinds' website. These were basic representations relating to: (i) the NIST Cybersecurity Framework, (ii) role-based access controls, (iii) passwords, (iv) network monitoring, and (v) secure software development. My opinion, based on the extensive evidence I have reviewed, is that SolarWinds clearly implemented these practices in a manner consistent with the Security Statement. The contrary view of the SEC's expert is, in my opinion, the product of a misguided analysis that does not comport with any recognized methodology in the cybersecurity field.

2. My opinions are informed by my many years of cybersecurity experience across a variety of institutions, including the military, the federal government, and the private sector. Having conducted or overseen numerous cybersecurity assessments, I am very familiar with how such assessments are ordinarily done. An outside expert assessing whether a company has certain controls in place gathers information from people in the company who are knowledgeable about the controls in order to understand how they are designed, and looks for artifacts generated from the operation of those controls to ensure that they were implemented.

3. I applied these standard practices in assessing whether SolarWinds implemented the practices at issue in the Security Statement. I reviewed the sworn testimony of SolarWinds employees describing how the company implemented these practices, and I reviewed large volumes of artifacts from the implementation of the practices that corroborated the testimony. This is similar to what I would do if I had been hired to do an assessment of SolarWinds' compliance with the Security Statement in a non-litigation context. What I reviewed is exactly the sort of

evidence I would expect to see from a company implementing the practices described in the Security Statement, and it easily leads me to the conclusion that the relevant portions of the Security Statement were accurate.

4. I have also reviewed the report of the SEC’s proffered expert, Mark G. Graff. I find both Mr. Graff’s methodology and his substantive conclusions to be deeply flawed. Instead of considering the large volume of direct evidence demonstrating SolarWinds’ implementation of the practices at issue, he appears to have considered only a small number of documents concerning marginal, one-off incidents or issues, and concludes, without significant explanation, that they are “suggestive” of “systemic” failures. They are not. The documents he cites generally have little to do with the practices described in the Security Statement at all. But in any event they certainly do not demonstrate any systemic failure to implement the practices at issue, nor do they somehow negate all of the evidence showing that the practices were in fact implemented, which Mr. Graff ignores. Accordingly, nothing in Mr. Graff’s report changes any of my opinions.

II. QUALIFICATIONS

5. I have over 30 years of experience in cybersecurity, both as a practitioner and an academic, having served in various cybersecurity roles in government and private institutions and companies—including as Director of Cybersecurity on the National Security Council at the White House and as the Chief Information Security Officer (“CISO”) of JPMorgan Chase. Throughout my career, I have managed cyber defense organizations and systems, prevented and responded to various cyber threats and incidents, and established and overseen large cybersecurity programs and operations.

6. Currently, I am a Partner at Next Peak, LLC, a cybersecurity consulting company that I co-founded in 2019. In my consulting practice, I work with a range of commercial and governmental clients to scrutinize their cybersecurity programs in an effort to understand gaps and

to help improve their cybersecurity posture and mitigate cyber risks. These engagements typically include assessments that draw on well-established industry frameworks, such as the NIST Cybersecurity Framework (“CSF”), the International Standards Organization (“ISO”) 27000 series of standards, and the Center for Internet Security (“CIS”) security controls. My teams also assist our clients in conducting penetration testing and red team exercises, both of which involve structured testing efforts to find flaws and vulnerabilities in IT defenses.

7. Additionally, I am the Chief Strategy and Risk Officer for Andesite AI, an early-stage company focused on the improvement of cybersecurity operations through advanced data science and artificial intelligence. I also serve as the Executive Director of the Cyber Defense Assistance Collaborative, an initiative to coordinate voluntary support of over twenty leading technology companies to provide cybersecurity assistance to the Ukrainian government and critical infrastructure companies within the country. I also advise Red Cell Partners, a venture capital fund, with its cyber investment practice. Finally, I am an adjunct senior research professor at Columbia University’s School of International and Public Affairs, where I co-teach a course on the fundamentals of cyber conflict, oversee various academic initiatives related to cybersecurity, and publish my work in the field.

8. From 2014 to 2019, I was Chief Information Security Officer & Head of Global Cyber Partnerships at JPMorgan Chase, where I directed its cyber defense program and oversaw more than 1,000 personnel and a \$500 million budget. My responsibilities included policy and program development and implementation, cyber and data security operations, and response and regulatory compliance. This included oversight of JPMorgan Chase’s data protection program. I also led the establishment of various advanced cybersecurity operations, such as the company’s insider threat program, red team program, and other cyber exercise programs.

9. Prior to my work in the private sector, I served in the United States Air Force for

27 years, reaching the rank of Colonel, and focusing on intelligence and cybersecurity. In the course of my military career, my responsibilities included the protection of systems, personnel, and facilities from inadvertent disclosure of data and foreign espionage activities. I also served as Director of Cybersecurity within the National Security Council at the White House, where I worked to ensure the cybersecurity of all U.S. government agencies and to promote public-private partnerships for national defense. I was a principal author of “The National Strategy to Secure Cyberspace,” signed by President George W. Bush in 2003, which was a public report that helped define the United States’ cybersecurity strategy at the time. I also coined the term “advanced persistent threat,” now widely used to describe state-sponsored cyber threat actors, in the course of my work helping the government to defend its systems against such threat actors.

10. In 1984, I earned a Bachelor’s in Science from the U.S. Air Force Academy in both Political Science and Military History. Subsequently, I received a Master of Public Policy with a concentration in International Affairs and Security from the John F. Kennedy School of Government at Harvard University in 1986. Ultimately, I received a Ph.D. in International Security from the Fletcher School of Law and Diplomacy at Tufts University in 1998. There, I wrote my dissertation, “Strategic Warfare in Cyberspace,” which was subsequently published by MIT Press in 2001.

11. In my capacity as a professor at Columbia University and in various other roles, I have published numerous academic articles and other works related to international security, national security, and cyber risk management. A complete list of my written works is available in my CV, which is attached as Appendix A to this Report.

12. I have testified on two occasions as an expert within the last four years. The information for those cases is provided in Appendix B to this Report.

III. INSTRUCTIONS

13. I have been retained on behalf of Defendants SolarWinds and Tim Brown as an independent expert in connection with this matter. Specifically, I have been asked to review certain representations made on a page on SolarWinds' website describing its basic security practices (the "Security Statement"). I understand that the Securities & Exchange Commission ("SEC") has alleged that these representations were false or misleading during the time period from SolarWinds' initial public offering, which occurred on October 19, 2018, to January 12, 2021 (the "Relevant Period"). I have been asked to opine on whether, based on the evidence available to me, these representations were true—that is, whether SolarWinds had practices in place during the Relevant Period that align with these representations. I provide my opinions on this issue in Part V of this Report.

14. I have also been asked to review the report prepared by the SEC's proffered cybersecurity expert, Mark G. Graff (the "Graff Report"), and to provide my opinions as to the validity of the conclusions that he reaches. I provide those opinions in Part VI of this Report.

15. A list of the documents I considered in formulating my opinions is attached as Appendix C to this Report.

16. My hourly rate for work on this matter is \$1,100/hour.

IV. METHODOLOGY

17. I have many years of experience with cybersecurity assessments and have conducted or overseen scores of such assessments over the course of my career. In arriving at my opinions in this case, I have sought to approximate the methodology that I (and other cybersecurity experts) apply in conducting an external assessment of whether an organization has certain cybersecurity controls in place.

18. Specifically, in conducting such an assessment, it is standard practice to do the

following:

- a. Interview key employees and management with knowledge of the controls and how they are implemented.
- b. Collect and review documentation concerning how these controls are implemented on a day-to-day basis, including both written policies as well as artifacts that are generated in practice through the operation of the controls.
- c. Leverage the results of any relevant outside cybersecurity audits to understand what they previously observed in relation to the controls.

19. To the extent I observe any gaps where I would expect to find documentation, I do not simply assume there is an absence of such evidence. Instead, standard practice for me—and in my opinion, any reasonable assessment—is to identify these gaps for the company and ask if there are materials that would fill those gaps, or, if the materials do not exist, ask for an explanation of why that is the case, so that I can incorporate those facts into my assessment.

20. By the same token, if any of the materials I review raise questions about possible deficiencies in the relevant controls, I do not simply stop there and draw a negative conclusion. Instead, I seek to understand the context for that information and how it fits into the broader picture of other materials and information I have received. My follow-up may include, for example, consulting with employees who are knowledgeable about the materials to better understand them. That, too, is standard practice in conducting a cybersecurity assessment.

21. Although my assignment in this matter is of course different in some respects than a standard security assessment, I tried to follow a similar approach as much as I could in arriving at my opinions. Specifically, I took the following steps:

- a. I reviewed the representations in the Security Statement that are challenged in the SEC's Amended Complaint, which are essentially the “controls” that I undertook to

“assess.”

b. I reviewed the deposition testimony of SolarWinds employees in this matter, which contained information about how the practices described in the Security Statement were implemented—information similar to what I would seek to obtain through employee interviews in an ordinary assessment (with one helpful difference being that, here, the information was even provided under oath).

c. I asked for, and was provided and reviewed, documentary evidence relating to the practices at issue, including SolarWinds’ written policies regarding these practices, as well as artifacts generated through the implementation of these practices on a day-to-day basis.

d. I compared the witness testimony and the documentary evidence regarding the practices to determine if they align with the representations about them in the Security Statement, interpreting those representations as I believe they would be understood in the industry, based on my extensive cybersecurity experience.

22. This approach reasonably approximates a standard external cybersecurity assessment that I might perform as an expert in the field, and it provided me with facts that were more than sufficient for me to form opinions about the accuracy of the representations in the Security Statement at issue.

V. THE REPRESENTATIONS IN THE SECURITY STATEMENT ACCURATELY DESCRIBE SOLARWINDS’ PRACTICES DURING THE RELEVANT PERIOD

23. From my review of the SEC’s complaint, I understand the SEC’s overarching allegation to be that “[t]he Security Statement was materially misleading because it touted the Company’s supposedly strong cybersecurity practices.” Specifically, the SEC alleges the Security Statement made false or misleading misrepresentations about five topics:

- a. the NIST Cybersecurity Framework (“NIST CSF”);
- b. role-based access controls;

- c. passwords;
- d. network monitoring; and
- e. secure software development.

24. Below I first explain why, in my view, the SEC is wrong to conceive of the Security Statement as “touting” that SolarWinds had “strong cybersecurity practices.” In reality, the Security Statement was merely designed to answer routine cybersecurity diligence questions from customers and most of the practices it describes are rather basic.

25. Against this context, I then go on to analyze each of the challenged portions of the Security Statement and explain why, based on my review of the evidence, they accurately describe SolarWinds’ practices during the Relevant Period.

A. The Security Statement Merely Describes SolarWinds’ Basic Security Practices

26. The Security Statement was posted to SolarWinds’ website in late 2017. Around that time, it was becoming more common for companies to put cybersecurity vendor diligence requirements in place, requiring their procurement departments to conduct cybersecurity diligence on their software vendors. In part, this was driven by expanding regulatory requirements around cybersecurity, including the EU’s General Data Protection Regulation, which imposed a broad set of new privacy and security rules on any companies doing business in the EU, and which many companies were preparing to comply with in the leadup to May 2018, when it was scheduled to go into effect.

27. Companies would often organize their vendor diligence efforts by ranking their vendors into different tiers of criticality—based on how important each vendor was to the company’s business and what level of access it had to the company’s data—and then applying different levels of diligence for the different tiers. So, for a vendor in a low-criticality tier, a company might only require confirmation that the vendor has certain basic cybersecurity practices

in place—confirmation they might obtain by sending the company a brief questionnaire or by finding the needed information on the company’s website. By contrast, for a vendor in a high-criticality tier, a company would do more extensive diligence, often sending the vendor a lengthy questionnaire with dozens or even hundreds of questions about specific requirements, potentially implicating sensitive details about the company’s cybersecurity practices that would not be suitable to post on a website.

28. Based on witness testimony, the Security Statement was designed to answer basic questions from customers about SolarWinds’ security.¹ As Tim Brown explained, it was a high-level FAQ that would allow a company conducting light diligence of SolarWinds to tick a “checkbox” denoting that it had cybersecurity practices in place.² In other words, the Security Statement was designed for customers that considered SolarWinds to be a low-criticality vendor. The information in the Security Statement was not detailed enough to meet the more demanding diligence required by customers that considered SolarWinds to be a high-criticality vendor. As witnesses testified, those customers would send SolarWinds detailed questionnaires requesting information going beyond what was in the Security Statement, which SolarWinds would provide only under an NDA.³

29. In light of this context, I disagree with the SEC’s characterization of the Security

¹ T. Brown Dep. Tr. at 292:17-20 (explaining that the statements in the Security Statement are “very basic” and “would be met by most companies”); *see also* E. Quitugua Dep. Tr. at 84:7-10 (explaining that purpose of Security Statement was “to help our customers and potential customers get just a very quick glance at whether or not we did some kind of security”); R. Johnson Dep. Tr. at 67:13-25 (indicating the purpose was to “summarize SolarWinds’ security – basic security practice”).

² T. Brown Dep. Tr. at 74:10-17 (explaining that purpose of Security Statement was to allow a SolarWinds customer to “get through some of the third-party risk processes that just require a baseline set of knowledge, you know, a checkbox that says, yes, they [i.e., SolarWinds] have a security statement”).

³ *Id.* at 81:7-82:22 (explaining that SolarWinds had an “NDA version of the security statement” it would use to answer “detailed security questionnaires” that some customers would have); E. Quitugua Dep. Tr. at 87:15-22 (“When customers or potential customers asked, Okay, well, I saw your security statement on the website, I have more questions, ... we had a process by which we would enter into an agreement, an NDA agreement, with the potential customer to—so that we could describe in more detail some of the practices described in our public-facing statement”).

Statement as “touting” that Solar Winds had particularly “strong” cybersecurity controls in place.⁴ That is not what the Security Statement says or what it was for. Many of the practices described in the Security Statement are basic practices that one would expect to find at any sizable software company. This is consistent with the purpose of the document, which was only to provide customers with basic information about SolarWinds’ cybersecurity practices, for customers who were only looking for that level of information to complete their cybersecurity diligence.

B. The Security Statement’s Representation About Following the NIST Framework Was Accurate

30. I understand that the SEC challenges the representation in the Security Statement concerning the NIST Cybersecurity Framework or “NIST CSF.” That representation simply states that “SolarWinds follows the NIST Cybersecurity Framework with layered security controls to help identify, prevent, detect and respond to security incidents.”⁵ Based on the evidence I have reviewed, the statement was true.

31. The NIST CSF is a resource issued by the National Institute for Standards and Technology, which is housed within the U.S. Department of Commerce. First published in 2014, the NIST CSF is a self-evaluation framework designed to be broadly useful for all manner of companies, regardless of their level of size or sophistication. As it states: “While the Framework has been developed to improve cybersecurity risk management as it relates to critical infrastructure, it can be used by organizations in any sector of the economy or society. It is intended to be useful to companies, government agencies, and not-for-profit organizations regardless of their focus or size.”⁶

⁴ Am. Compl. ¶ 7.

⁵ SW-SEC00466129 (SolarWinds’ Security Statement).

⁶ *Framework for Improving Critical Infrastructure Cybersecurity Ver. 1.1* (“NIST CSF 1.1”), NIST (Apr. 16, 2018) at 3, <https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf>. Version 1.1 of NIST was the version in place during the Relevant Period.

32. In line with this objective, the focus of the NIST CSF is on *process*, not *substance*. That is, it does not set forth a substantive set of cybersecurity standards or requirements that a company must implement in order to “comply.” Rather, it sets forth a framework for companies to use in evaluating their cybersecurity programs, in order to identify improvements they wish to make against their current baseline, based on their own priorities, constraints, and risk appetites.

33. The introduction to the NIST CSF makes this clear. As it explains, instead of imposing requirements, it “provides a common taxonomy and mechanism” for self-assessment, designed to help organizations:

- 1) Describe their current cybersecurity posture;
- 2) Describe their target state for cybersecurity;
- 3) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
- 4) Assess progress toward the target state;
- 5) Communicate among internal and external stakeholders about cybersecurity risk.

Likewise, the NIST CSF stresses the flexibility it is intended to provide:

The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances. They also will vary in how they customize practices described in the Framework. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks.⁷

34. The framework set forth in the NIST CSF is simple. It divides cybersecurity activities into five broad layers, called “Functions,” labeled: “Identify,” “Prevent,” “Detect,” “Respond,” and “Recover.”⁸ Within each Function, the framework lists categories and

⁷ *Id.* at vi.

⁸ *Id.* at 3.

subcategories of cybersecurity objectives, such as the category “Asset Management” within “Identify,” and the subcategory under it: “Physical devices and systems within the organization are inventoried.”⁹ A company using the NIST CSF is supposed to rate itself under each category, by selecting a numerical score—or “Tier”—for its controls in each category. As the NIST CSF states: “Tiers describe an increasing degree of rigor and sophistication in cybersecurity risk management practices.”¹⁰

35. Importantly, a company following the NIST CSF is not required to meet any particular Tier. The Tiers are not meant to serve as passing or failing grades. Rather, “[t]iers are meant to support organizational decision making about how to manage cybersecurity risk, as well as which dimensions of the organization are higher priority and could receive additional resources. Progression to higher Tiers is encouraged when a cost-benefit analysis indicates a feasible and cost-effective reduction of cybersecurity risk.”¹¹ By going through this process of self-evaluation, a company obtains a clearer picture of its baseline cybersecurity posture, or “Current Profile,” and what it needs to do to determine the state it wants to achieve, or “Target Profile.”

36. Following the NIST CSF does not entail adhering to any strict or formal procedure. As the NIST CSF states: “To account for the unique cybersecurity needs of organizations, there are a wide variety of ways to use the Framework. The decision about how to apply it is left to the implementing organization.”¹² Thus, while the NIST CSF includes a list of categories and subcategories of cybersecurity activities that a company may evaluate itself on, it also makes clear that companies are free to select which of these categories or subcategories to use, or to add others

⁹ *Id.* at 23–24.

¹⁰ *Id.* at 8.

¹¹ *Id.*

¹² *Id.* at vi.

not listed, based on the organization's unique needs and requirements.¹³ Similarly, while the NIST CSF includes four Tiers and a set of definitions for each, organizations can customize those definitions or use their own scoring methodologies.¹⁴ "The Framework is voluntary, so there is no 'right' or 'wrong' way to do it."¹⁵

37. The essence of following the NIST CSF is for an organization to have a recurring process for evaluating its cybersecurity in order to guide decisions about where to improve and how to allocate resources. Fundamentally, it is a tool for cybersecurity governance. As the NIST CSF states:

[The NIST CSF's] five high-level Functions will provide a concise way for senior executives and others to distill the fundamental concepts of cybersecurity risk so that they can assess how identified risks are managed, and how their organization stacks up at a high level against existing cybersecurity standards, guidelines, and practices. The Framework can also help an organization answer fundamental questions, including "How are we doing?" Then they can move in a more informed way to strengthen their cybersecurity practices where and when deemed necessary.¹⁶

38. Based on the evidence I have reviewed, it is clear that SolarWinds followed the NIST CSF as a framework for self-evaluation. Ironically, this is reflected in the very documents

¹³ See *id.* at 22 ("Activities can be selected from the Framework Core during the Profile creation process and additional Categories, Subcategories, and Informative References may be added to the Profile. An organization's risk management processes, legal/regulatory requirements, business/mission objectives, and organizational constraints guide the selection of these activities during Profile creation.").

¹⁴ See, e.g., *NIST Cybersecurity Framework 2.0: Quick-Start Guide for Using the CSF Tiers*, NIST (October 2024), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1302.pdf>, at 2 ("An organization wanting to use the CSF Tiers can reuse the notional descriptions from Appendix B of the CSF, or they can customize those descriptions, create new ones, or use a set of descriptions they already have in place."). For the "NIST Scorecards" that it created during the Relevant Period, see *infra*, SolarWinds, which is based in Austin, Texas, appears to have borrowed descriptions from a variation of the NIST CSF issued by the Texas state government. *Compare Texas Cybersecurity Framework*, Texas Dep't of Information Resources (last visited Nov. 22, 2024), <https://dir.texas.gov/information-security/security-policy-and-planning/texas-cybersecurity-framework> with SW-SEC00001497 at -505 (describing NIST "Maturity Level[s]" 0-5).

¹⁵ *Cybersecurity Framework 1.1 Components*, NIST (Feb. 6, 2018), <https://www.nist.gov/cyberframework/cybersecurity-framework-components>. Mr. Brown testified to having a similar understanding at his deposition. See T. Brown Dep. Tr. at 191:14-21 ("Q. Does NIST CSF say that you should just use an arithmetic average for the various security categories to come up with the overall rating for Identify, Protect, Detect, Respond, and Recover? A. I believe what it says is that you should use this as a maturity model. And how you grade yourself is up to you. There's not a direct tie to any specific model to be used.").

¹⁶ NIST CSF 1.1 at 14.

that the SEC cites in its Amended Complaint as evidence that SolarWinds supposedly did *not* follow the NIST CSF. Specifically:

a. As early as August 2017, Eric Quitugua, who headed SolarWinds’ InfoSec Team, prepared “an assessment of the state of our security program” that he sent to Tim Brown, then SolarWinds’ Vice President of Security and Architecture, shortly after he arrived at the company. As Mr. Quitugua stated in the email, the assessment was based on “security controls mapped to the NIST Cybersecurity framework.”¹⁷ The spreadsheet attached to the email reflects a set of security categories organized under the five NIST Functions as to which Mr. Quitugua had assigned numerical scores.¹⁸

b. Likewise in October 2018, Mr. Quitugua sent Mr. Brown a spreadsheet titled “SolarWinds Security Program Assessment,” which contained a set of security categories organized under the five NIST Functions as to which Mr. Quitugua had assigned numerical scores.¹⁹

c. In August 2019, SolarWinds’ Chief Information Officer, Rani Johnson, and Mr. Brown started a practice of including “NIST Scorecards” in periodic presentations to management.²⁰ These evaluations contained a set of security categories organized under the five NIST Functions, as to which Ms. Johnson and Mr. Brown assigned numerical scores.²¹ As Ms. Johnson and Mr. Brown both explained in their deposition testimony, the scores were meant to

¹⁷ SW-SEC00350067 (cited in Am. Compl. at ¶ 79).

¹⁸ SW-SEC00350069 (cited in Am. Compl. at ¶ 79).

¹⁹ SW-SEC00013678 (cited in Am. Compl. at ¶ 83).

²⁰ See SW-SEC00001497 at -498 (noting agenda includes “Introduc[ing] Security Score Card”) (cited in Am. Compl. ¶ 89).

²¹ See R. Johnson Dep. Tr. 152:7-15 (noting that she, Mr. Brown, and Ms. Pierce “curated content from different departments to aggregate this quarterly meeting”); *id.* at 162:11-21 (explaining that the NIST scores were “an assessment based on ... the collective aggregate of the assessments that were being performed. ... It was math. You summarize the answers from the different security assessments to form a formulaic score.”); T. Brown Dep. Tr. at 223:19-21 (“If a program had completed or a major advancement had been done, we would have updated the score.”).

draw management’s attention to areas they were seeking to improve, in order to keep management informed of how cybersecurity risk was being managed and to drive allocation of resources to where they were needed—exactly what NIST CSF evaluations are designed to do.²²

d. The inclusion of NIST Scorecards in presentations to management continued into 2020.²³ The scores showed a trend of continuing improvement across all of the NIST CSF Functions from 2017 to 2020.²⁴ Again, part of the purpose served by the NIST CSF is to help a company plan and measure its improvement over time.

39. I therefore have no difficulty in concluding that SolarWinds followed the NIST CSF. The company used the NIST CSF on a recurring basis as a tool for self-evaluation, in order to identify opportunities for improvement, guide decisions about how to allocate resources, and communicate information about cybersecurity risk to stakeholders. That is what the NIST CSF was designed for, and that is what “following” the NIST CSF entails.

C. The Security Statement’s Representations About Role-Based Access Controls Were Accurate

40. I understand that the SEC challenges the representations in the Security Statement concerning role-based access controls. Those representations state as follows:

Role Based Access

Role based access controls are implemented for access to information systems. Processes and procedures are in place to address employees who are voluntarily or

²² See T. Brown Dep. Tr. at 90:10-20 (“[T]he NIST Cybersecurity Framework ... is a framework that allows companies ... flexibility in how they measure their security programs, and it’s meant to be a measurement to allow you to look at where you are from the program perspective and then improve upon it. It’s one of the ... things that we read out to and have read out to the executive team as far as our NIST CSF status.”); *id.* at 281:16-24 (“16 Q. How would management know exactly what issues, uh, you were concerned about in any of these slides [i.e., NIST Scorecards], for example, the access controls issues that were at issue with respect to the one score that you were asked about? A. So we would verbally discuss those scores and we would focus on those low scores. And the discussion would lead to, So, Rani, what programs have you started? How are we going to move this up?”); R. Johnson Dep. Tr. at 161:12-23 (explaining that NIST Scorecards were “a summary for us to assess our general maturity ... against the outlined objectives”); 219:1-17 (“[T]his [i.e., the NIST Scorecard] was an awareness vehicle for leadership. ... We created this vehicle to summarize and provide awareness to other business departments.”).

²³ See, e.g., SW-SEC00001608 at -611 (“NIST Maturity Level” Scorecard); SW-SEC00001582 at -587 (same).

²⁴ *Id.*

involuntarily terminated. Access controls to sensitive data in our databases, systems, and environments are set on a need-to-know / least privilege necessary basis. Access control lists define the behavior of any user within our information systems, and security policies limit them to authorized behaviors.

Authentication and Authorization

...

SolarWinds employees are granted a limited set of default permissions to access company resources, such as their email, and the corporate intranet. Employees are granted access to certain additional resources based on their specific job function. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as defined by our security guidelines. Approvals are managed by workflow tools that maintain audit records of changes.²⁵

41. Based on the evidence I have reviewed, these statements were true.

42. Role-based access controls are measures designed to give users access only to those systems they need to perform their roles.²⁶ The language in the Security Statement describes how role-based access controls were implemented at SolarWinds. The evidence I have reviewed reflects that SolarWinds had processes and procedures consistent with these representations, which were designed to ensure that employees' access privileges were tailored to their roles and that their access was terminated when they left the company. There are large volumes of artifacts that reflect the implementation of these processes and procedures during the Relevant Period, consistent with testimony from multiple witnesses.

43. First, SolarWinds had an established process for categorizing each employee's role at the company and provisioning them with access privileges matched to that role. In onboarding a new employee, the employee's manager would fill out a form—known as a “System Access Request Form” or “SARF”—on which the manager would identify the employee's role at the

²⁵ See Am. Compl. ¶ 179; SW-SEC00466129 at -132.

²⁶ See, e.g., *Computer Security Resource Center, Glossary*, NIST (last visited Nov. 22, 2024), https://csrc.nist.gov/glossary/term/role_based_access_control (defining “role-based access control” as “[a]ccess control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role)”).

company. The company's IT department would then use the SARF to provision the employee with the access appropriate to that role. A similar process was used if an employee changed roles within the company during their period of employment and needed access to different systems: A SARF would be filled out identifying the new accesses needed and the IT department would implement the request. And when an employee was terminated, a similar process was used to shut off their access to SolarWinds resources. As Joe Kim, SolarWinds' Chief Technology Officer during the Relevant Period, testified:

What [the] SARF [process] was utilized for was ... when somebody would join the company, to be able to give them appropriate access to systems within your organization [i.e., the employee's team at the company] and make sure that you only had access to the areas that you should and not in areas that you should not. And then similar process, again, utilizing SARF, was followed for you to be able to do the same thing when you're changing from one job to another. ... And then if somebody was getting terminated, it would also go through the SARF process to make sure that you are—you know, your access was going away from any of the company systems.²⁷

44. I have reviewed samples from over a thousand SARFs I have received that were filled out for newly hired employees during the Relevant Period, evidencing they were completed as a regular practice.²⁸ Two samples, reflecting the SARF form as it existed from 2018 to mid-2019 and from mid-2019 to 2020, respectively, are provided as Exhibits A-1 and A-2 to this report.

a. As indicated on the first version of the form, there were dozens of different types of roles that were defined for purposes of provisioning employees with access rights.²⁹ For

²⁷ J. Kim Dep. Tr. at 79:4-19; *see* E. Quitugua Dep. Tr. at 326:8-15, 336:21-337:6 (explaining that a SARF was "basically a request form submitted to kick off the account provisioning process," and that after being filled out by the employee's manager, IT "got the form to process and created the accounts and set up the level of access and level of permission"); T. Brown Dep. Tr. at 204:21-205:3 ("We had a manual process to onboard and give appropriate access rights to people called S-A-R-F. And what that process was, was a process where somebody joined a company, went to HR. HR would send an email to IT with an appropriate rule and then those rules would say onboard this person in this way. Then if they needed additional privileges, they went through another process to be able to be granted additional privileges.").

²⁸ *See, e.g.*, SW-SEC-SDNY_00190582; SW-SEC-SDNY_00190776; SW-SEC-SDNY_00190995; SW-SEC-SDNY_00063051; SW-SEC-SDNY_00055459; SW-SEC-SDNY_00064179; SW-SEC-SDNY_00061206; SW-SEC-SDNY_00060927. The entire set I received is contained at: SW-SEC-SDNY_00059641–SW-SEC-SDNY_00065510.

²⁹ Exhibit A-1 at -236 ("Standard System Access for SolarWinds Employees").

each role, the form listed a standard set of systems that users within that role would receive access to—on top of company-wide systems (e.g., email) to which all employees would receive access. Where applicable, the form also specified a particular level of access within a system that was appropriate for a user in a particular role. For example, the 2018 form specifies the following access rights for someone in the “Marketing – Demand Generation” role³⁰:

Marketing – Demand Generation

Netsuite – SW Marketing Admin (upon request)
Salesforce.com - Marketing User
MicroSoft Vizio
Silverpop / Marketo
LiveBall

This indicates someone in this role would receive access to the applications listed—Netsuite, Salesforce.com, MicroSoft Vizio, Silverpop / Marketo, and LiveBall. It also indicates that, for Salesforce.com, the level of access granted would be that of a “Marketing User,” and for Netsuite, the level of access would be that of a “SW Marketing Admin,” if requested. For other roles, the form provided completely different lists of systems and privilege levels, such as in the following examples (out of many)³¹:

IT – Security Team

Netsuite – SW Helpdesk
Web Helpdesk – Tech access
Additional accesses to be requested based on role

Senior Finance (Controllers and Treasury)

Netsuite – Global Accountant & access corresponding to job duties
On-line banking – as approved
Solium Transcitive – Read Access (as approved)

R&D – QA & Testers

Netsuite – SolarWinds Support Person
Fogbugz / Jira
Active Directory – SWDEV account
Tableau – QA Managers & above
Perforce – upon request
Go to Meeting account – Managers & above
Testlink account
VM & vSphere

³⁰ *Id.*

³¹ *Id.*

b. The 2019-20 version of the SARF form was more automated. The systems and privilege levels associated with a particular role could be found through entering the employee's region, business, unit, function, and team in an online form, which would bring up the "role-defined accesses" that would be "provisioned for the new hire by default."³² For example, for an employee in the "IT Help Desk" function, in the "DOIT / Architecture / UX & Engineering" team, in the "G&A" business unit, the accesses listed would be as follows³³:

Application Portal	EIE Role	Permission Level	Provisioning Group
Active Directory	Employee	Standard User	EUS
SolarHR	Employee	Standard User	HR Ops
Saba	Employee	Standard User	HR Ops
Web HelpDesk	Employee	Standard User	Infrastructure Engineering
Confluence	Employee	Standard User	EUS
Coupa	On Request	Standard User	Business Applications
Office 365	Employee	Standard User	EUS
CIMS	Manager	Standard User	HR Ops
Bswift	Employee	Standard User	HR Comp
Egencia	VP + On Request	Standard User	Corporate Travel
JIRA	Employee	Standard User	Engineering Ops
Web HelpDesk	Employee	Help Desk: (L1) Access	Infrastructure Engineering
Exchange	Employee	Help Desk: (L1) Access	Infrastructure Engineering
Office 365	Employee	Help Desk: (L1) Access	Infrastructure Engineering

³² Exhibit A-2 at -068 ("System Access Provisioning via SARF 2.0").

³³ *Id.*

Access Rights Management	Employee	Standard User	
--------------------------	----------	---------------	--

The “Application / Portal” would be the resource granted access to; the “EIE role” would indicate the role (or special request) required to obtain the access listed; the “Permission Level” would be the level of privilege being granted within the resource; and the “Provisioning Group” would be the name for the group of users (or “access control list,” discussed further below) that the user would be added to on the relevant provisioning system in order to assign the user the listed access rights.

c. In addition to the standard access assignments that were defined for each role, the SARF (both versions of it) allowed the employee’s manager to specify any non-standard systems that the employee also needed access to. Absent such special approval, however, the employee would be limited to the standard systems designated for their role.³⁴

45. Once a SARF was completed, it would be sent to IT support personnel, who in turn would implement the system accesses requested. They would do this by generating “tickets” on SolarWinds’ IT help-desk platform, which would be directed to the personnel needed to provide the employee with access to the relevant systems. The tickets would specify what systems the employee needed to access and what level of access they needed on the systems. As Mr. Cline testified:

So the SARF ... would be filled out by a manager or an individual, depending on whether they’re being hired and onboarded or were already with the company. That SARF would flow through the ticketing system At that point multiple tickets would get generated, which, depending on the access or resources that were requested, it would go to different teams for implementation of those access levels.³⁵

³⁴ See, e.g., Exhibit A-1 at -235 (“For any system access required that is **non-standard**, please list the system and access level needed. ... All approvals for non-standard access should be documented and retained.” (emphasis in original)); Exhibit A-2 at -067 (same and documenting approval for non-standard system access).

³⁵ B. Cline Dep. Tr. at 42:17-43:3.

As with the SARF forms, I have reviewed samples from thousands of these tickets I have received from the Relevant Period, evidencing that they were generated as a regular practice as part of the SARF process.³⁶

46. As testified by Mr. Quitugua, at a technical level, an employee would be granted access to systems by adding them to the appropriate access control lists.³⁷ An access control list is simply a table of users with rules (or “policies”) specifying the permissions each user has on a given network or system. As both Mr. Quitugua and Mr. Cline testified, many resources on SolarWinds’ network were managed through Active Directory, which is a Microsoft service that is used to centrally manage users on a Windows-based network.³⁸ Thus, an employee in the Finance department could be added as a non-admin user to an access control list on Active Directory specifically for Finance users, which would give the employee non-administrative access to a set of financial systems managed through Active Directory.³⁹ Similarly, an HR

³⁶ See, e.g., SW-SEC-SDNY_00059189; SW-SEC-SDNY_00049602; SW-SEC-SDNY_00049688; SW-SEC-SDNY_00049716; SW-SEC-SDNY_00050052; SW-SEC-SDNY_00051207; SW-SEC-SDNY_00051423; SW-SEC-SDNY_00051811; SW-SEC-SDNY_00051672. The entire set of help-desk tickets for onboarding requests I received is contained at: SW-SEC-SDNY_00049599–SW-SEC-SDNY_00051840 (SARF onboarding help-desk request tickets from October 30, 2017 through June 6, 2019 produced from WebHelpDesk, with SARF forms attached) and SW-SEC-SDNY_00051842 (spreadsheet listing over 20,000 SARF tickets—including both onboarding requests and other types of SARF requests—dating from May 31, 2019 through January 12, 2021, produced from IT ServiceDesk); see also SW-SEC-SDNY_00189217–SW-SEC-SDNY_00191598 (SARF forms relating to IT ServiceDesk tickets).

³⁷ E. Quitugua Dep. Tr. at 326:19-24 (“The SARF form described exactly what level of access your job required of you. That form—the request then gets to the IT team, who is responsible for creating the accounts and adding it to the user access lists that were made – or managed through Active Directory.”); *id.* at 338:6-18 (“[T]he hiring manager defined what roles the new employee or their direct report needed access to or, you know, what resources. That determined what groups—what user access lists that new employee would be—become a member of. ... [The SARF] would be sent to the IT to configure the settings or add that account to the respective groups that were already set in [A]ctive [D]irectory.”); B. Cline Dep. Tr. at 46:1-3 (explaining that SolarWinds had “very granular groups” for different “roles” within the company).

³⁸ E. Quitugua Dep. Tr. at 325:12-18 (explaining that Active Directory was the “primary means” SolarWinds used to manage user access lists); B. Cline Dep. Tr. at 46:1-6, 89:21-90:2 (“Active directory is the server that handles in particular your user identity in connection to that specific domain ...”).

³⁹ E. Quitugua Dep. Tr. at 327:17-328:2 (“Q. Yeah. You mentioned user access or access control lists I think is the term you used. What does that have to do with this process? A. So say you were hired as a finance team member, your account based on your hiring—the hiring manager’s request for access would be added to a very specific group for finance. If you were in HR, you would be added to an HR group. And what that did—or does is it only grants you the least level of privilege that's required for you to do your work.”).

employee could be added as a non-administrative user to an access control list for HR users, which would give the employee non-administrative access to HR-related systems managed through Active Directory.⁴⁰ For systems that were not managed through Active Directory to which an employee needed access, the relevant system owners would need to add the employee to access control lists specific to those systems.

47. SolarWinds also had special controls in place for provisioning users with administrative access to sensitive systems, i.e., access that allowed a user to manage or configure servers, applications, databases, or similar resources on the network. Not only would such access need to be requested through the SARF process, but also the network monitoring that SolarWinds did through its Security Event Manager or “SEM” (discussed below⁴¹) would detect if any user were added as an administrator to a system. In that event, the SEM (also called a “log and event manager” or “LEM”) would send an alert to the InfoSec team, which would check to ensure that the granting of access was appropriate. As Mr. Cline testified:

Q. ... And can you just briefly walk me through the ticketing process ... for a request for administrative privileges starting in 2018?

A. Yes, ma'am. It was very specific to ... what we considered administrative roles within our server environment, application environment or security network environment. And so all of those roles had very granular groups within our Active Directory ... [I]f someone requested access to a particular group they needed with their job to do, let's say, [network] switch administration[,] [t]hat group that they would get access to was logged and monitored by the LEM or SEM, and any alerts that an addition or change was made there would go to the InfoSec team ...

[T]hey would ask us, Is there a reason why this change was made[,] and we would respond back with the corresponding ticket that needed to be there or the reason why we elevated that account.⁴²

⁴⁰ *Id.*

⁴¹ See *infra* at Section V.E.

⁴² B. Cline Dep. Tr. at 45:20-47:3; see also E. Quitugua Dep. Tr. at 336:21-337:21 (explaining that the InfoSec team would receive an alert if heightened privileges were added to a user's account, which would lead the InfoSec team to confirm that there was a “business justification” for the change); SW-SEC-SDNY_00054914 (internal document

48. I have reviewed a sample from more than 100 email chains I received relating to these alerts, from dates across the Relevant Period.⁴³ The emails show SolarWinds' InfoSec team being alerted of a user being added to an administrator group, and then confirming that the action was "authorized and intentional," by conferring with others or by finding the corresponding help-desk ticket approving the change. These emails confirm that SolarWinds had this additional process in place to ensure that network administrative privileges were limited to those who needed them to perform their role, consistent with Mr. Cline's testimony and the representations in the Security Statement.

49. The SARF process was also used to request any *changes* to an employee's access to system resources—such as granting an employee access to additional systems, or increasing their level of privilege within a system, if their role at the company changed. A SARF requesting the change would be prepared and submitted to IT support staff, which would generate workflow tickets that would track confirmation of any approvals needed for the requested changes and implementation of the changes. Again, I have samples from numerous SARFs I received requesting such changes, along with corresponding tickets, evidencing that this practice was commonly followed during the Relevant Period.⁴⁴

50. Offboarding of an employee would be handled in a similar fashion. The employee's manager would prepare a SARF designating the employee for termination. The SARF would then be sent to IT support personnel, who would generate tickets in SolarWinds' workflow

listing the types of events that would result in "[e]mail alerts sent from SEM to InfoSec for investigation," which included the enabling of an admin account or the addition of a user to a security group).

⁴³ See, e.g., SW-SEC-SDNY_00054778; SW-SEC-SDNY_00054780; SW-SEC-SDNY_00054787; SW-SEC-SDNY_00054829; SW-SEC-SDNY_00054835; SW-SEC-SDNY_00054791; SW-SEC-SDNY_00054794; SW-SEC-SDNY_00054786; SW-SEC-SDNY_00054831. The entire set I received is contained at: SW-SEC-SDNY_00115556–SW-SEC-SDNY_00115781.

⁴⁴ See, e.g., SW-SEC-SDNY_00055454; SW-SEC-SDNY_00055458; SW-SEC-SDNY_00047323; SW-SEC-SDNY_00047368; SW-SEC-SDNY_00047441; SW-SEC-SDNY_00047734; SW-SEC-SDNY_00047783. The entire set I received is at: SW-SEC-SDNY00047304–SW-SEC-SDNY_00047791. I understand that the tickets have been produced with the corresponding SARF forms attached.

software that would track the deprovisioning of the employee's access and note when it was completed. Again, I have reviewed samples from numerous SARFs I received requesting such changes, along with corresponding tickets, evidencing that this practice was commonly followed during the Relevant Period.⁴⁵

51. SolarWinds also had formal policy documentation describing how the SARF process worked, titled "User Access: Standard Operating Procedure." The document explains how SolarWinds managed user access through the SARF process.⁴⁶ The procedure described in the policy is consistent with the SARFs and tickets I have reviewed.

52. All of these are the sorts of artifacts I would look for had I been hired in an ordinary business context to conduct an assessment of SolarWinds' role-based access controls. In my opinion they easily demonstrate that the representations in the Security Statement relating to role-based access controls were true.

a. The first three sentences state:

Role based access controls are implemented for access to information systems. Processes and procedures are in place to address employees who are voluntarily or involuntarily terminated. Access controls to sensitive data in our databases, systems, and environments are set on a need-to-know / least privilege necessary basis.⁴⁷

Again, the purpose of the SARF process was to ensure that access to information systems was "role based" and set on a "need-to-know" or "least privilege necessary" basis. Users would receive a defined set of access rights based on their specific role and any greater access rights required specific managerial approval. The company also used SEM alerts for any granting of network

⁴⁵ See, e.g., SW-SEC-SDNY_00056418; SW-SEC-SDNY_00056480; SW-SEC-SDNY_00056264; SW-SEC-SDNY_00056152; SW-SEC-SDNY_00056183; SW-SEC-SDNY_00056189; SW-SEC-SDNY_00056213; SW-SEC-SDNY_00056218; SW-SEC-SDNY_00056268. The entire set I received is at: SW-SEC-SDNY_00047792–SW-SEC-SDNY_00049598. I understand that the tickets have been produced with the corresponding SARF forms attached.

⁴⁶ See SW-SEC00218161 (August 2019 version); SW-SEC00042771 (2018 version).

⁴⁷ SW-SEC00466129 at -132.

administrative privileges to ensure they were needed for a user's role. As to the termination of employees, the SARF process addressed the deprovisioning of employees' access when they were terminated.

b. The next sentence states:

Access control lists define the behavior of any user within our information systems, and security policies limit them to authorized behaviors.⁴⁸

This simply describes how access rights would have been managed at a technical level—by adding or removing users to or from access control lists for the relevant systems. As explained above, this is how requests made through the SARF process were implemented.

c. The remaining sentences state:

SolarWinds employees are granted a limited set of default permissions to access company resources, such as their email, and the corporate intranet. Employees are granted access to certain additional resources based on their specific job function. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as defined by our security guidelines. Approvals are managed by workflow tools that maintain audit records of changes.⁴⁹

This again describes what happened in the SARF process: All employees were given a limited set of default permissions to company-wide resources, but beyond that any additional access was dependent on their role or individual need based on managerial approval. And the granting of access was managed through workflow tools that maintained records of the changes made—namely, the help-desk tickets that were generated by IT personnel to track implementation of the access requested on a SARF form.

53. While the foregoing by itself allows me to conclude that the representations in the Security Statement regarding access controls were true, it is also important to note that SolarWinds conducted regular reviews of user access rights—referred to internally as “user access reviews” or

⁴⁸ *Id.*

⁴⁹ *Id.*

“UARs”—to ensure that employees did not have access inappropriate to their role. As multiple witnesses testified, these user access reviews were completed on a regular basis by the IT team, which would inventory user access control lists on key systems, to confirm that access privileges were appropriately assigned—and to catch any potential errors that might be made in the provisioning process.⁵⁰ I have reviewed samples from over 50 user access reviews that I received, dating from various times across the Relevant Period, evidencing that they were prepared as a regular practice.⁵¹ The reviews appear to go through all of the active accounts on various systems used by the team being reviewed, in order to confirm that each account was still needed by an active employee and to identify any accounts for former employees that may have been missed during the deprovisioning process. These reviews were an additional layer of control designed to ensure that users were provisioned with access based on their role and that processes were in place to address terminated employees, consistent with the Security Statement.

⁵⁰ See R. Johnson Dep. Tr. at 78:23-25 (“User access reviews were conducted on a regular basis to determine whether or not access was appropriate.”); B. Cline Dep. Tr. at 123:8-124:20 (explaining that the company did “account audits” on a “regular basis” throughout the year); E. Quitugua Dep. Tr. at 342:3-344:5 (stating that “user access reviews” were conducted during the Relevant Period, in order “to make sure that access controls were being implemented appropriately”); T. Brown Dep. Tr. at 110:5-8 (stating that the IT department conducted, in addition to the process for onboarding and offboarding employees, “user access reviews” as part of their procedures “to determine who should have access to what”).

⁵¹ See, e.g., SW-SEC00296522 (Q1 2019 Mail Assure UAR); SW-SEC00296398 (Q2 2019 AppOptics UAR); SW-SEC00296424 (Q2 2019 Papertrail UAR); SW-SEC00296385 (Q3 2019 Loggly UAR); SW-SEC00147804 (Q4 2019 Pingdom UAR); HOLTZMAN_0000395 (Q1 2020 Loggly UAR); SW-SEC00221545 (Q2 2020 Automated Net License UAR); SW-SEC00235950 (Q3 2020 RMM UAR); SW-SEC00148226 (Q4 2020 Backup UAR); SW-SEC00148013 (Q1 2021 Backup UAR). The entire set I received is at: SW-SEC00147725–SW-SEC00147726; SW-SEC00147804–SW-SEC000147806; SW-SEC00148016; SW-SEC00148225–SW-SEC00148226; SW-SEC00148235; SW-SEC00148248; SW-SEC000148265; SW-SEC00206893; SW-SEC00208525; SW-SEC00212505–SW-SEC000212506; SW-SEC00212978–SW-SEC000212982; SW-SEC00221223; SW-SEC0022576; SW-SEC00296399; SW-SEC00296459–SW-SEC00296462; SW-SEC00296464; SW-SEC00296477–SW-SEC00296480; SW-SEC00296488; SW-SEC00296492–SW-SEC00296495; SW-SEC00296521–SW-SEC00296523; SW-SEC00296929; SW-SEC00296939–SW-SEC000296941; SW-SEC00296945; SW-SEC00296972; SW-SEC00297948; SW-SEC00297950–SW-SEC00297951; SW-SEC00297953; SW-SEC00297964–SW-SEC00297967; SW-SEC00297975; SW-SEC00298003; SW-SEC00298074–SW-SEC00298075; SW-SEC00298077–SW-SEC00298079; SW-SEC00508346; SW-SEC00508766; SW-SEC00533902; SW-SEC00539561; SW-SEC00572180; SW-SEC00648173–SW-SEC00648174; SW-SEC00648177–SW-SEC00648178; SW-SEC00648446–SW-SEC00648447; SW-SEC00648450–SW-SEC00648451; HOLTZMAN_0000656; HOLTZMAN_0000658; HOLTZMAN_0004209; HOLTZMAN_0005932; HOLTZMAN_0009420; HOLTZMAN_0011780; PWC-SEC-00036809; PWC-SEC-00045839–PWC-SEC-00045840; PWC-SEC-00045843–PWC-SEC-00045844; PWC-SEC-00046476; PWC-SEC-00046530.

54. Finally, and again importantly, my opinion that SolarWinds implemented role-based access controls as described in the Security Statement is consistent with the results of multiple outside audits of SolarWinds during the Relevant Period. These include (1) annual SOX audits, relating to the company’s compliance with Sarbanes-Oxley requirements for financial reporting and (2) SOC-2 Type II audits, which are security-related attestations that SolarWinds obtained for certain of its products.

55. First, SolarWinds was subject to SOX audits in 2019 and 2020, conducted by outside auditor PricewaterhouseCoopers (“PwC”). SOX audits include audits of a company’s “IT General Controls” or “ITGCs,” which are controls on a company’s network that relate to the security of systems used in financial reporting. The scope of these ITGC audits performed by PwC encompassed various SolarWinds IT systems that SolarWinds and the auditor determined to be related to financial reporting—which, as I know from reviewing the work papers from these audits, included Active Directory, the primary system SolarWinds used to manage users on its network.

a. The work papers I have reviewed indicate that the controls audited with respect to these in-scope systems included the following⁵²:

2.0	User Access Policy	A user access management policy is established and documented for initiating, authorizing, recording, processing, reviewing a request for access rights, and evidence retention. The user access management policy is reviewed and approved annually by the VP of IT. Evidence of review is documented and retained.
2.2	Access Provisioning	New users are provisioned access in accordance with the SolarWinds System Groups Matrix. Any additional access required, including access to super user or admin responsibilities, require approval from manager, IT and/or the system owner. Additional NetSuite access to sensitive worldwide financial results requires approval by the Financial Controller or the VP of WW Finance.
2.3	Termination	When an employee is terminated, access to Active Directory and financial systems is removed in a timely manner, as follows: - within 24 hours for administrator access - within 7 days for all other levels of access

⁵² See PWC-SEC-00028649 (2020 PWC audit work papers, overview tab listing controls tested); PWC-SEC-00017450 (2019 PWC audit work papers, “Control description” column in each tab describing controls tested).

2.5	Access Reviews	User access privileges are re-validated on a quarterly basis to confirm that users maintain appropriate access. These validation procedures are performed for all financially significant applications, systems (including Active Directory users) and databases.
-----	----------------	---

b. Some of these controls go above and beyond the basic role-based access controls described in the Security Statement, but these controls are consistent with and encompass the controls described in the Security Statement. For example, the statement that “[a] user access management policy is established and documented for initiating, authorizing, recording, processing, reviewing a request for access rights, and evidence retention” roughly maps onto the representations in the Security Statement describing the SARF process. Likewise, the statements explaining that new users were provisioned based on a matrix of user groups (like the matrix found in the SARF), and that “[a]ny additional access required, including super user or admin responsibilities, require approval from manager, IT and/or the system owner,” map onto the representations in the Security Statement about how users are granted limited access rights based on their role and that additional access rights require special approvals.

c. The work papers indicate that PwC audited these controls by reviewing samples of documentation relating to access provisioning, including documentation from the SARF process and the user access reviews that SolarWinds periodically conducted.⁵³

d. I know from my experience with such audits that, had SolarWinds lacked the above controls, or failed to implement them in any systemic way, PwC would have issued a “material weakness” finding in connection with SolarWinds’ ITGCs during the Relevant Period, which the company would have to have noted in its annual SEC filings. PwC made no such finding. Thus, to the extent PwC found any exceptions in the above controls, it did not consider them to be material.

⁵³ See PWC-SEC-00028649 (2020 PWC audit work papers with tab for each control explaining testing done); PWC-SEC-00017450 (2019 PWC audit work papers with tab for each control explaining testing done).

56. Additionally, during the Relevant Period, SolarWinds engaged several outside assessors to conduct SOC-2 audits relating to several SolarWinds product lines.⁵⁴ SOC-2 audits are cybersecurity assessments that are sometimes sought by software customers for assurance that a software vendor has appropriate security controls in place. While the SOC-2 audits prepared for SolarWinds were specific to certain product lines, they specifically found that role-based access controls were implemented for the systems that were within the scope of the assessments—further evidencing that such controls were consistently implemented across the organization.

a. For example, a SOC-2 report prepared by auditor Lurie, LLP for SolarWinds' Passport, Documentation Manager, Blink, and Site applications, dated November 15, 2019, stated:

SolarWinds has implemented role-based security to limit and control access within the in-scope systems and supporting tools. Employees are granted logical and physical access to in-scope systems based on documented approvals by employee managers. The ability to create or modify user access accounts and user access privileges is limited to users whose job responsibilities require such access. ... Administrative access to servers and databases is restricted to users whose job responsibilities require such access.⁵⁵

b. Similarly, a SOC-2 report prepared by auditor Holtzmann Partners, LLP for SolarWinds' Loggly application, dated December 31, 2019, found the following assessment criteria to be satisfied:

CC6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

⁵⁴ See, e.g., HOLTZMAN_0003092 (Holtzman Partners, LLP Dec. 31, 2019 SOC-2 Report for Loggly application); HOLTZMAN_0001016 (Holtzman Partners, LLP Jan. 17, 2020 SOC-2 Report for AppOptics application); HOLTZMAN_0001823 (Holtzman Partners, LLP Oct. 31, 2020 SOC-2 Report for Loggly application); LURIE0010117 (Lurie, LLP Mar. 31, 2020 SOC-2 Report for Pingdom application); LURIE0010269 (Lurie, LLP Mar. 31, 2020 SOC-2 Report for Database Performance Monitoring System); LURIE0010230 (Lurie, LLP Nov. 15, 2019 SOC-2 Report for Password and Documentation Management System).

⁵⁵ LURIE0010230 at -247.

CC6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.⁵⁶

57. Accordingly, I have no difficulty in concluding that the Security Statement's representations concerning access controls were accurate. The representations describe a set of processes and procedures designed to ensure that employees were provisioned with access rights that were limited to what they needed to perform their role. There is an abundance of artifacts evidencing that the described processes and procedures were in place—the same sorts of artifacts that I would look for had I been hired as an outside consultant to do an assessment of SolarWinds' controls, and the same sorts of artifacts that *were* reviewed by external firms that conducted SOX audits and SOC-2 assessments for SolarWinds, who found the controls to be in place.

D. The Security Statement's Representations About Passwords Were Accurate

58. I understand that the SEC challenges the representations in the Security Statement concerning passwords. Those representations state as follows:

We require that authorized users be provisioned with unique account IDs. Our password policy covers all applicable information systems, applications, and databases. Our password best practices enforce the use of complex passwords that include both alpha and numeric characters, which are deployed to protect against unauthorized use of passwords.⁵⁷

59. Based on the evidence I have reviewed, these statements were true.

1. Unique User IDs

⁵⁶ HOLTZMAN_0003092 at -108.

⁵⁷ SW-SEC00466129 at -132. The Security Statement also stated: "Passwords are individually salted and hashed." "Hashing" and "salting" refer to cryptographically protecting passwords in databases used to check user credentials when users log in. I do not address this representation as Mr. Graff does not address it in his report. Moreover, while the SEC alleges at one point in the Amended Complaint that certain passwords were not "salted and hashed," the facts described there relate to hard-coding passwords in plain text in server configuration files, which is not the same thing as failing to salt and hash passwords in a credentials database. Am. Compl. ¶ 166. Configuration files are different from credential databases, and it would make no sense to store a hashed and salted password in a configuration file. While the Security Statement said nothing about whether SolarWinds hard-coded passwords in configuration files, I address this issue below in responding to Mr. Graff's report. *See infra* Section VI.D.2.

60. The first sentence—“We require that authorized users be provisioned with unique account IDs”—does not itself relate to passwords, but rather simply indicates that SolarWinds provisioned users on its network with unique usernames. Evidence of SolarWinds following this practice is found in the user access reviews that SolarWinds conducted, which list individual users along with their usernames. Again, I have reviewed a sample of these user access reviews selected at random from across the Relevant Period.⁵⁸ They consistently list a unique username for each individual user listed, typically consisting of their first and last name separated by a dot, or else some other variation of the user’s name, such as their first initial followed by their last name. This is as one would expect, as users need unique user accounts to be able to maintain their work files and data separately from other users.

2. Written Password Policy

61. The second sentence in the above paragraph states: “Our password policy covers all applicable information systems, applications, and databases.” To my understanding, this sentence simply represented that SolarWinds had a written password policy, which covered all systems, applications, and databases within SolarWinds’ network environment. This was true. SolarWinds had a policy document titled “Enterprise Information Security Guidelines,” which defined various security controls that were required to be in place across SolarWinds’ environment. For example, version 1.4 of the document, from November 8, 2017, contained the following guidance relating to password complexity:

3.7. Passwords cannot contain the user’s account name or parts of the user’s full name that exceed two consecutive characters.

3.7.1. Passwords must be at least 8 characters in length.

3.7.2. Passwords must contain characters from three of the following four categories:

⁵⁸ See *supra* note 51 and accompanying text.

3.7.3.English uppercase characters (A through Z).

3.7.4.English lowercase characters (a through z).

3.7.5.Base 10 digits (0 through 9).

3.7.6.Non-alphabetic characters (for example, !, \$, #, %).⁵⁹

Subsequent versions of the policy document have similar guidance.⁶⁰

62. I have also reviewed materials reflecting that SolarWinds employees were specifically instructed on the company’s password policy. For example, I have reviewed a set of security training slides that were provided to SolarWinds employees at onboarding, which included a slide setting forth SolarWinds’ password policy.⁶¹ This is further evidence that SolarWinds had a password policy and sought to make users aware of it.

3. Enforcement of Password Complexity

63. The third sentence in the quoted paragraph from the Security Statement—“Our password best practices enforce the use of complex passwords that include both alpha and numeric characters, which are deployed to protect against unauthorized use of passwords”—speaks to the issue of automatic enforcement of password complexity. There are essentially two ways that a company can seek to ensure that employees use complex passwords. It can do so manually, by instructing employees on the criteria passwords need to meet and relying on them to follow that criteria in choosing their passwords. Or the company can *enforce* password complexity

⁵⁹ SW-SEC00302590 at -592-93.

⁶⁰ See, e.g., SW-SEC00303137 (version 1.5); SW-SEC00639163 (version 2.0). I note that Mr. Graff asserts that SolarWinds only had a policy applicable to “financially significant” systems, but he cites a different document—titled “User Access Process Narrative”—which appears to have been created for SOX audit purposes. See Graff Report ¶ 134 n.250 (citing SW-SEC00223527). Mr. Graff ignores the Enterprise Information Security Guidelines the company had in place, which were not limited to financial systems. See J. Bliss Dep. Tr. at 305:10-20 (testifying that the Enterprise Information Security Guidelines was SolarWinds’ “written password policy”); see also R. Johnson Dep. Tr. 205:18-25 (explaining that SolarWinds had “access control guidelines” and that “all critical assets were assessed against those guidelines”).

⁶¹ See, e.g., SW-SEC00012076 at -079 (discussing “[p]assword policy”); SW-SEC00285599 at -603 (same); SW-SEC00156433 at -435 (same).

automatically, through technical constraints that block attempts to create a password that does not conform to set criteria.

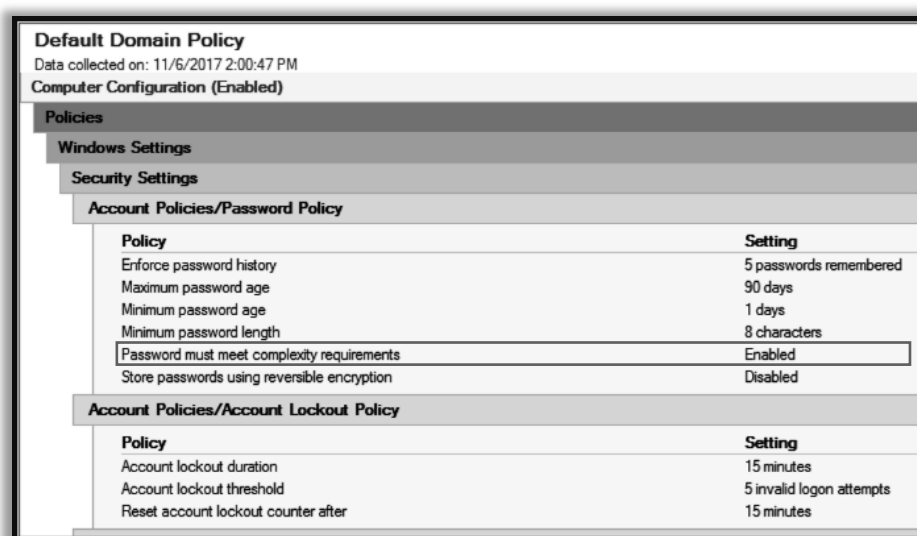
64. Obviously, automatic enforcement is preferable—hence the reference in the Security Statement to it being a “best practice”—but it is only an option where the system at issue allows for it. For example, a law firm can configure its own network to automatically enforce complex passwords for user accounts on the network. But its lawyers may also need to access an external application, like LEXIS or Westlaw, using separate credentials. The law firm may not be able to automatically enforce its own password requirements on such applications because it does not control those applications, and the applications may not provide a feature that allows a corporate customer to set password requirements for its employees who use the applications. The application providers, like LEXIS or Westlaw, may have their own, different password requirements, or may not have any password requirements at all.

65. Given this context, my understanding of the Security Statement’s representation that SolarWinds’ “best practices” were to “enforce the use of complex passwords” is that SolarWinds automatically enforced password complexity through technical measures where it was feasible to do so. This understanding is consistent with an internal policy document I have reviewed, titled “User Access Process Narrative,” which explains SolarWinds’ password practices for purposes of SOX audits (which cover financially significant systems). As it states:

The Company maintains password requirements for all financially significant systems (including Active Directory, NetSuite, ADP, Activation Server, Zuora, and SolarHR) and databases (SQL License Orchestration database), including the requirements that they be changed periodically, meet minimum length requirements, retain password history, and require password complexity, **as allowed by the application, system, or database**. If access is limited by a password and requires log in through Active Directory (including system accounts), specific password requirements are not considered necessary as password

*password configuration settings for Active Directory are enforced.”*⁶⁵

67. There is clear evidence in the record that SolarWinds did enforce password complexity on Active Directory. In particular, I have reviewed a chat between Tim Brown and Eric Quitugua from November 6, 2017, in which Mr. Brown asked Mr. Quitugua “what our password rules are on AD”—i.e., Active Directory.⁶⁶ Mr. Quitugua sent Mr. Brown the following screenshot of the “Account Policies/Password Policy” settings that were in place for Active Directory at the time⁶⁷:



Default Domain Policy	
Data collected on: 11/6/2017 2:00:47 PM	
Computer Configuration (Enabled)	
Policies	
Windows Settings	
Security Settings	
Account Policies/Password Policy	
Policy	Setting
Enforce password history	5 passwords remembered
Maximum password age	90 days
Minimum password age	1 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled
Account Policies/Account Lockout Policy	
Policy	Setting
Account lockout duration	15 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	15 minutes

68. As indicated in the screenshot, “Password must meet complexity requirements” was enabled. Per Microsoft guidance at the time, this was a “best practice” and meant that:

- passwords could not contain the user’s account name or parts of a user’s full name (i.e., first name, middle name, last name), provided the part was more than two letters long; and
- passwords were required to contain characters from three of the following categories:
 - Uppercase letters
 - Lowercase letters

⁶⁵ SW-SEC00251041 at -041 (emphasis added).

⁶⁶ SW-SEC-SDNY_00055078.

⁶⁷ SW-SEC-SDNY_00055077 (red outlining added).

- Base 10 digits (0 through 9)
- Nonalphanumeric characters: ~!@#\$%^&* _-+=`|(){}[];":'<>.,?/
- Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase.⁶⁸

In other words, the effect of this setting was to enforce precisely the password complexity requirements listed in SolarWinds internal policy documentation, as described above in ¶ 61.

69. I have also reviewed external audits reflecting that outside auditors repeatedly found that SolarWinds implemented its password policy, including password complexity requirements.

a. First, the SOX audits that PwC performed encompassed user access controls for Active Directory and other systems considered financially significant, and the audits included the following control⁶⁹:

2.1	Access Provisioning	The Company <i>maintains password requirements</i> for all financially significant systems and databases, including the requirements that they be changed periodically, meet minimum length requirements, retain password history, <i>and require password complexity, as allowed by the application, system, or database.</i> Web hosted applications may not require active directory authentication. If access is limited by a password and requires log in into Active Directory (includes system accounts) the requirements for password change, password complexity and password history are not considered necessary.
-----	---------------------	--

Based on the PwC work papers I have reviewed, access to most of the applications PwC examined was managed through Active Directory, which PwC noted was configured to enforce password complexity requirements. Accordingly, PwC found that the password configuration design for these systems were “appropriately designed.”⁷⁰ For systems that had their own “system-specific password policy,” apart from Active Directory, PwC generally determined that password

⁶⁸ See *Password must meet complexity requirements*, Microsoft (Nov. 27, 2017), [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh994562\(v=ws.11\)](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh994562(v=ws.11)).

⁶⁹ See PWC-SEC-00028649 (2020 PwC audit work papers at “Overview” tab) (emphasis added); PWC-SEC-00017450 (2019 PwC audit work papers at “2.1 Password Settings” tab) (emphasis added).

⁷⁰ PWC-SEC-00017450 (2019 PwC audit work papers at tab “2.1 Password Settings,” Rows 17-23); see also PWC-SEC-00028649 (2020 PwC audit work papers at tab “2.1 Password Settings,” Rows 22-165 (noting that controls were “designed effectively”)).

configuration design was appropriate for these systems as well.⁷¹ As noted above, if PwC had observed any systemic failure to implement password complexity requirements, it would have issued a “material weakness” finding as to SolarWinds’ ITGCs. The fact that it did not do so indicates that it was satisfied the requirements were materially in place.

b. Second, the SOC-2 audits issued for SolarWinds included assessments of password controls on systems used in connection with the development of the products being assessed. These reports found that these systems had “been configured to enforce (1) a user ID for login, (2) minimum password length, (3) password complexity, (4) password expiration, and (5) password non-reuse restrictions.”⁷² Notably, the systems assessed included systems outside Active Directory. For example, the SOC-2 report issued for SolarWinds’ Loggly application focused on an Amazon Web Services (“AWS”) environment used to support the Loggly application, and found that the company had used “AWS’ Identity and Access Management” functionality to enforce the foregoing password controls on the AWS login console used by SolarWinds developers.⁷³

70. In short, as with role-based access controls, I have no difficulty in concluding that the Security Statement accurately described SolarWinds’ practices with respect to passwords. Users were provisioned with unique account IDs, as evidenced by user access reviews listing those account IDs; the company had a written password policy, as evidenced by the policy itself; and, as a “best practice,” the company automatically enforced complex passwords where it was feasible

⁷¹ *Id.* PwC only found two minor exceptions relating to the password control they assessed, neither of which related to a failure to enforce password complexity, and neither of which were deemed to be a “significant deficiency,” let alone a “material weakness.” See PWC-SEC-00044562 (“FY2019 Deficiencies and Recommendations” spreadsheet at tab “IT Deficiencies,” Rows 7 and 25, at column I (describing the two exceptions), at column J (classifying each as a “control deficiency” (“CD”) which is the least serious form of deficiency in a SOX audit), and at column M (explaining “[w]hy the impact is not pervasive”)).

⁷² HOLTZMAN_0003092 at -103; HOLTZMAN_0001823 at -834; HOLTZMAN_0001016 at -027.

⁷³ HOLTZMAN_0003092 at -103 (“The console and command-line interface (CLI) are secured through AWS’ Identity and Access Management ...”).

to do so, as evidenced by the password complexity setting that was enabled on Active Directory and multiple outside audits validating that password complexity controls were in place.

E. The Security Statement’s Representations About Network Monitoring Were Accurate

71. I understand that the SEC has challenged certain representations in the Security Statement it characterizes as relating to “network monitoring,” as follows:

Change Management

Changes to information systems, network devices, and other system components, and physical and environment changes are monitored and controlled through a formal change control process. Changes are reviewed, approved, tested and monitored post-implementation to ensure that the expected changes are operating as intended.

Auditing and Logging

Network components, workstations, applications and any monitoring tools are enabled to monitor user activity.

Network Security

Our infrastructure servers reside behind high-availability firewalls and are monitored for the detection and prevention of various network security threats Next generation firewalls deployed within the data center as well as remote office sites monitor outbound communications for unusual or unauthorized activities⁷⁴

72. Based on the evidence I have reviewed, these statements were true.

1. Change Management

73. As to the statements under “Change Management,” they do not actually relate to “network monitoring” as that term is typically used in the industry. “Network monitoring” typically refers to live monitoring of events on a network, e.g., events like a user logging on to their account or accessing a particular system. “Change management,” by contrast, refers to the process of rolling out configuration changes to systems on a network—such as upgrading network software or applying security patches to systems. Such changes can cause unexpected glitches

⁷⁴ Am. Compl. ¶ 148; *see also* SW-SEC00466129 at -130-31.

that, in some circumstances, can lead to significant technology outages or business disruptions. (An extreme example would be the CrowdStrike software update released in July 2024, which caused a glitch when it was installed by CrowdStrike customers that led to major outages at airlines and many other companies.⁷⁵) For this reason, companies put “change management” processes in place to ensure that such changes are planned and tested before being rolled out, and monitored while they are rolled out, so that any glitches can be caught before causing any significant issues.

74. Those sorts of processes are what the “Change Management” language in the Security Statement concerns. Putting aside they have little to do with “network monitoring,” the evidence I have reviewed reflects that SolarWinds had such processes in place. As Mr. Cline explained at length at his deposition: SolarWinds had a “formal change control process” in which proposed changes were made through “[C]hange [M]anagement [R]equests” or “CMRs,” which would be tracked and managed on SolarWinds’ internal IT ticketing system.⁷⁶ A CMR would explain the scope and details of the change being proposed.⁷⁷ Before being implemented, the change would first require approval by a manager, and then approval by a “Change Administration Board” or “CAB,” composed of “representatives from each major IT team” at the company, who met once a week “to discuss and review changes of a medium or high impact.”⁷⁸ If a change was approved by the CAB, the relevant IT team would roll out the change, monitoring for any problems, and initiating a rollback if a significant problem was detected.⁷⁹ Once the change was

⁷⁵ See, e.g., M. Suer, *CrowdStrike’s Critical Flaw: When Change Management Fails, So Does Trust*, CMSWire (Aug. 22, 2024), <https://www.cmswire.com/customer-experience/crowdstrikes-critical-flaw-when-change-management-fails-so-does-trust/>.

⁷⁶ B. Cline Dep. Tr. at 55:12-23; see also *id.* at 42:6-17 (“We used [a ticketing system] for our change management tracking and a large piece of that was what we called our CMRs or a change management request.”).

⁷⁷ *Id.* at 57:11-58:11 (“We would have an initial creation of the CMR scoping out all of its details of the scope of the change ...”).

⁷⁸ *Id.* at 43:5-14, 55:12-56:22, 57:11-23 (“[The CMR] would get reviewed by the manager, approved by the manager and then get discussed at the [Change Administration Board] meeting.”).

⁷⁹ *Id.* at 63:5-65:24 (“So if the change was a failure, they would implement their rollback process and that was just a standard – standard part of implementing a change.”).

completed and it was confirmed that there was no negative impact, the CMR ticket would be closed.⁸⁰ The processes described by Mr. Cline are entirely consistent with those described in the “Change Management” section above.

75. Further, I have reviewed samples from more than 700 CMR tickets that I understand from speaking with Mr. Cline were retrieved from the relevant internal ticketing systems used by SolarWinds during the Relevant Period.⁸¹ The tickets reflect that changes to network infrastructure were planned, tested, and monitored as Mr. Cline testified. I have also reviewed what I understand from speaking with Mr. Cline are a sample of calendar invites from across the Relevant Period for CAB meetings. These invites contain links to documents about upcoming or closed-out changes that it appears were to be reviewed at each meeting. The invites corroborate that changes were reviewed and approved by the CAB, as Mr. Cline testified.⁸²

2. Auditing and Logging

76. As to the representation under “Auditing and Logging”—that “[n]etwork components, workstations, applications and any monitoring tools are enabled to monitor user activity”—I understand this to mean that SolarWinds configured systems on its network to generate logs of user activity so that the activity could be audited or monitored for anomalous events. A best practice for such monitoring is to configure network systems to generate logs and to send the logs in real time to a centralized monitoring solution, known as a Security Information and Event Management solution, or “SIEM,” so that the network can be broadly monitored on a

⁸⁰ *Id.* at 58:19-21 (“[O]nce the change was completed and confirmed that there was no impact, then the ticket would get closed.”).

⁸¹ *See, e.g.*, SW-SEC-SDNY_00052397; SW-SEC-SDNY_00052470; SW-SEC-SDNY_00052671; SW-SEC-SDNY_00052380; SW-SEC-SDNY_00052500; SW-SEC-SDNY_00052634; SW-SEC-SDNY_00052659; SW-SEC-SDNY_00052670; SW-SEC-SDNY_00052663; SW-SEC-SDNY_00052644; SW-SEC-SDNY_00052673. The entire set I received is contained at: SW-SEC-SDNY_00051843–SW-SEC-SDNY_00052673.

⁸² *See, e.g.*, SW-SEC-SDNY_00055404 (1/16/2018); SW-SEC-SDNY_00055402 (5/3/2018); SW-SEC-SDNY_00055396 (10/18/2018); SW-SEC-SDNY_00055406 (11/1/2018); SW-SEC-SDNY_00055398 (3/7/2019); SW-SEC-SDNY_00055408 (8/8/2019); SW-SEC-SDNY_00055393 (1/16/2020); SW-SEC-SDNY_00055327 (12/3/2020).

real-time basis.

77. Based on the evidence I have reviewed, that is what SolarWinds did. SolarWinds itself offered a SIEM solution as one of its products during the Relevant Period, known as “Security Event Manager,” or “SEM”⁸³—which it also used to monitor its own network. Mr. Cline explained at his deposition that, as part of the company’s change management process, “if [SolarWinds] brought a new server or application online, that was something that we were to inform the InfoSec team on so that they could add it to the [SEM] And so they would add those systems into those event managers to collect those logs.”⁸⁴ Mr. Brown, who supervised the InfoSec team, testified similarly:

[M]any systems went into our Security Operations Center and the Security Operations Center operated [a] log[] [and] event management system powered by one of SolarWinds’ products. Essentially, that system collected logs from many different devices and stored those logs, [and] could highlight alerts for certain log entries that may indicate, you know, a threat coming in from the outside against a firewall. So my team was responsible for maintaining and monitoring that system.⁸⁵

Mr. Quitugua likewise testified that SolarWinds used its own log and event manager to “monitor event logs coming in” from “end points like workstations, servers and network devices.”⁸⁶

78. Further, I have reviewed a sample of reports, from various dates scattered across the Relevant Period, that I understand from speaking with Mr. Brown were generated by the SEM solution SolarWinds operated on its own network.⁸⁷ The reports reflect that tens of millions of events (and often over 100 million events) were logged by the SEM on a daily basis—events such

⁸³ See *Security Event Manager*, SolarWinds.com (last visited Nov. 22, 2024), <https://www.solarwinds.com/security-event-manager>.

⁸⁴ B. Cline Dep. Tr. at 71:5-72:6.

⁸⁵ T. Brown Dep. Tr. at 98:5-14.

⁸⁶ E. Quitugua Dep. Tr. at 21:5-14.

⁸⁷ See, e.g., SW-SEC-SDNY_00065704; SW-SEC-SDNY_00067944; SW-SEC-SDNY_00068243; SW-SEC-SDNY_00068765; SW-SEC-SDNY_00065806; SW-SEC-SDNY_00067639; SW-SEC-SDNY_00068840; SW-SEC00123922. The entire set I received is contained at: SW-SEC-SDNY_00065513–SW-SEC-SDNY_00069495 (Database Maintenance Reports).

as users logging on, applications being started, or files being read.⁸⁸ The reports also reflect that a portion of these events were security-related events, indicating that SolarWinds had configured the SEM to specifically log types of events relevant to security monitoring.⁸⁹ Thus, these reports confirm that SolarWinds configured systems on its network to be logged and monitored using its SEM solution, as Mr. Cline, Mr. Brown, and Mr. Quitugua all testified, and consistent with the Security Statement's representation that "[n]etwork components, workstations, applications and any monitoring tools [we]re enabled to monitor user activity."⁹⁰

3. Network Security

79. Finally, the language the SEC quotes from the Security Statement under the heading "Network Security" concerns the use of "[n]ext generation firewalls" that were "monitored for the detection and prevention of various network security threats."⁹¹ "Firewalls" are network-security devices that monitor and control traffic flowing to and from a network, or to and from internal zones within a network. They can be configured to block or alert on traffic that fits certain criteria, such as traffic from a blacklisted IP address. "Next-generation firewalls" have many capabilities that ordinary firewalls do not, which allow them to inspect traffic based on an extensive set of criteria that is constantly updated based on threat-intelligence feeds from external vendors. As one

⁸⁸ The reports label these "alerts," but the application uses this term simply to refer to "events." *See Documentation for Security Event Manager, Glossary of SEM Terms*, SolarWinds.com (last visited Nov. 22, 2024), https://documentation.solarwinds.com/en/success_center/sem/content/admin_guide/glossary-sem-terms.htm, at definition of "event" ("In SEM, the terms event and alert are interchangeable."). The SEM application allows rules to be set up that determine when certain events/alerts will result in the application taking responsive action, which can include sending email notifications to security personnel. *See Documentation for Security Event Manager, Create Rules that Respond to Security Events*, SolarWinds.com (last visited Nov. 22, 2024), https://documentation.solarwinds.com/en/success_center/sem/content/admin_guide/10-sem_rules/chapter-head-sem-rules.htm. SolarWinds had such rules in place, such as the automatic email notifications that the InfoSec team would be sent in the event that a user was given new administrative privileges. *See supra* ¶¶ 47-48 and accompanying footnotes.

⁸⁹ *See, e.g.*, SW-SEC-SDNY_00069121 at -121 (Database Maintenance Report showing 142,171,698 "Security Alerts").

⁹⁰ SW-SEC00466129 at -131.

⁹¹ Am. Compl. ¶ 148.

explanatory website puts it, if an ordinary firewall is like an airport security agency that checks passengers against a simple no-fly list (akin to a list of blacklisted IP addresses), next-generation firewalls are like an airport security agency that also inspects what items the passengers are carrying, looks for suspicious behaviors as they approach the gate, reviews intelligence databases for any derogatory information on the passengers, and so on.⁹²

80. Based on the evidence I have reviewed, SolarWinds did in fact use next-generation firewalls to monitor its network for threats. Mr. Cline testified extensively to this at his deposition. As he explained, the company used next-generation firewalls run by Palo Alto, a well-regarded cybersecurity vendor, not only to monitor traffic coming into SolarWinds' network from the outside, but also to monitor traffic between hundreds of segmented internal zones that SolarWinds maintained within its network:

We had a couple hundred different zones that would be broken down between offices, within an office, within a device type. And each one of those zones had their own rules regarding what type of traffic could transition from that zone to another zone. And that's where the firewall rules would come into place. ... And at that point in time the firewall ... looked at [user] behavior heuristically. If it saw anything [ab]normal from a data transmission or session standpoint, it would shut down that session and trigger an alert that went to the InfoSec team.

...

We had a subscription with Palo Alto to what was called WildFire, a subscription service that they provided where they were watching globally all of their firewalls across all of their companies and if they saw something suspicious happening in one region, they would send out a heuristical imprint that would get fed to all your devices so that it would also look for that behavior in your region and flag it.

That flag, how we handled that in normal standard process in our business was that would alert to the InfoSec team and the network team for review so that they could go and look to see what something might be malicious happening within our environment.⁹³

⁹² See *What Is a Next-Generation Firewall?*, Cloudflare Learning Center (last visited Nov. 9, 2024), <https://www.cloudflare.com/learning/security/what-is-next-generation-firewall-ngfw/>.

⁹³ B. Cline Dep. Tr. at 187:5-24, 189:16-190:5.

Mr. Brown testified similarly, explaining that “one of the things that [the InfoSec team] did was look at all of the events and alerts that came through firewalls ... to say is there anything suspect here that I should look at, anything suspect here that I should review?”⁹⁴

81. I have reviewed a sample of “InfoSec Daily Monitoring Reports” from over 700 that I received, taken from various dates across the Relevant Period.⁹⁵ I understand from speaking with Mr. Brown that these reports would be generated for the InfoSec team’s use on a daily basis by the Palo Alto next-generation firewalls SolarWinds used—as reflected by the “PaloAlto” logo at the bottom. The reports list various types of events detected on the firewalls that would be of potential interest to the InfoSec team, such as events involving the movement of large amounts of data (“500 MB File”), outbound traffic to a known malicious IP addresses that the firewall instead directed to a sinkhole (“DNS Sinkhole”), or SSH activity (used for remote logins or file-transfers) on a system port not typically used for such activity (“SSH on Non Standard port”).⁹⁶ These reports confirm that SolarWinds used next-generation firewalls to monitor its network for threats, consistent with Mr. Cline and Mr. Brown’s testimony, and consistent with the representations in the Security Statement.

82. In short, the evidence I have reviewed easily allows me to conclude that the sections of the Security Statement that the SEC groups under the heading “Network Monitoring” (erroneously, I should add, since change management is distinct from network monitoring) were accurate. SolarWinds had processes and procedures in place to plan, test, and monitor configuration changes; it fed system logs from across its network into its SEM solution, which

⁹⁴ T. Brown Dep. Tr. at 102:2-23.

⁹⁵ See, e.g., SW-SEC00048050; SW-SEC00055552; SW-SEC00080539; SW-SEC00568977; SW-SEC00110807; SW-SEC00568813; SW-SEC00080539; SW-SEC00056037; SW-SEC00073459; SW-SEC00105664; SW-SEC00049183. The bates numbers for the entire set I received are not in any sequential order; however, I understand they can be found in the discovery produced in this matter by searching for the title of the documents: “InfoSec Daily Monitoring Reports.”

⁹⁶ See, e.g., *id.*

monitored those logs for security events; and it used next-generation firewalls to monitor network traffic for security threats. All of these practices align with the corresponding descriptions in the Security Statement.

F. The Security Statement’s Representations About Software Development Were Accurate

83. Finally, I understand the SEC challenges the section of the Security Statement concerning SolarWinds’ software development lifecycle. That section states:

Software Development Lifecycle

We follow a defined methodology for developing secure software that is designed to increase the resiliency and trustworthiness of our products. Our products are deployed on an iterative, rapid release development lifecycle. Security and security testing are implemented throughout the entire software development methodology. Quality Assurance is involved at each phase of the lifecycle and security best practices are a mandated aspect of all development activities.

Our secure development lifecycle follows standard security practices including vulnerability testing, regression testing, penetration testing, and product security assessments. The SolarWinds architecture teams review our development methodology regularly to incorporate evolving security awareness, industry practices and to measure its effectiveness.⁹⁷

84. Based on the evidence I have reviewed, these statements were true. I first explain how I interpret the above two paragraphs, and then I explain the evidence I have reviewed that leads me to believe they were true.

85. The first paragraph speaks generally to the software development methodology followed by the company. As multiple witnesses testified, SolarWinds followed an “Agile” software development methodology.⁹⁸ In the software development field, Agile is a methodology defined in contrast to a “Waterfall” software development methodology. Specifically:

⁹⁷ SW-SEC00466129 at -132.

⁹⁸ See S. Colquitt Dep. Tr. at 25:21-26:8 (noting “SolarWinds use[s] a[n] Agile methodology” and “explain[ing] what an Agile methodology involves”); J. Kim Dep. Tr. at 119:12-22 (same); T. Brown Dep. Tr. at 124:14-125:17 (“[W]e had defined sprints for ... the development process. So it’s an Agile standard model of development of software.”).

a. A Waterfall methodology involves a linear approach where the components of building a piece of software are assigned to different teams in a sequential way, such that one component cannot proceed until the prior component is completed. For example, one team might build the database needed for the software, the next team might build the back-end system that processes data in the database, the next team might build the front-end system used by the user, and then the last team might be responsible for testing the completed product. The Waterfall methodology has the disadvantage of being slow and inflexible, and also, by pushing testing of software to the late stages of development, has the disadvantage of delaying discovery of bugs or security vulnerabilities until the end of the process, potentially requiring considerable work to be redone if significant problems are discovered at that point.⁹⁹

b. By contrast, the Agile methodology is iterative rather than linear. Rather than product development being broken up sequentially, with one team handing off development to the next, product development under the Agile methodology is broken up into compressed increments, called “sprints,” which each involve a cross-functional team working on various aspects of development at the same time. This allows the complete product to be assembled more quickly than in the Waterfall process. Also, product testing is not delayed until the end of the process, but rather is done as part of each iteration. In this way, potential flaws can be caught earlier in the process compared to the Waterfall methodology.¹⁰⁰

86. In this context, I understand the first paragraph of the “Software Development Lifecycle” section of the Security Statement to be representing that SolarWinds follows the Agile

⁹⁹ See, e.g., Antonio Nieto-Rodriguez, *It's Time to End the Battle Between Waterfall and Agile*, Harvard Business Review (Oct. 10, 2023), <https://hbr.org/2023/10/its-time-to-end-the-battle-between-waterfall-and-agile> (explaining disadvantages of Waterfall approach, including “the repercussions of late-stage testing, a characteristic of the Waterfall model”); Eric Perlman, *Agile vs. Waterfall: Which Delivery Approach is Right for You?*, Veritas Total Solutions (last visited Nov. 22, 2024), <https://info.veritasts.com/insights/agile-vs.-waterfall> (explaining how “Agile addresses the issues with waterfall delivery”).

¹⁰⁰ *Id.*

methodology rather than the Waterfall methodology to developing software. As it states, “products are deployed on an iterative, rapid release development lifecycle”¹⁰¹—which is a hallmark of the Agile methodology. Likewise, the paragraph states that security or quality assurance testing is done “throughout” or “at each phase” of the software development lifecycle,¹⁰² which I interpret to mean that such testing occurs as part of each iteration of software development, which is another hallmark of the Agile methodology, as opposed to the Waterfall methodology where such testing often does not occur until the end of the process.

87. The second paragraph quoted by the SEC provides further specifics about the security practices SolarWinds incorporated into its software development lifecycle. In particular, the first sentence—which I understand to be the SEC’s focus—states that SolarWinds’ software development lifecycle “follows standard security practices including vulnerability testing, regression testing, penetration testing, and product security assessments.”¹⁰³ Let me briefly explain what these terms mean:

a. The term “vulnerability testing” is commonly used to refer to the use of automated tools to scan code for vulnerabilities. These include (1) static analysis tools, which analyze the code as written, before it is run, to look for types of coding errors that are associated with known security vulnerabilities and (2) dynamic analysis tools, which analyze the software while it is running, to look for anomalous behaviors associated with known security vulnerabilities. There are many types of such tools on the market, which use varying technologies and vulnerability databases, and which can therefore produce varying results when run against the same code.

b. The term “regression testing” refers to testing changes in software to verify

¹⁰¹ SW-SEC00466129 at -132.

¹⁰² *Id.*

¹⁰³ See Am. Compl. ¶ 110.

that it still works as expected after the changes have been made. Regression testing is not security-specific—often the “regressions” found through such testing are simply degradations in the functionality of the software, but sometimes these bugs can have security implications.

c. The term “penetration testing” in the software development context refers to testing that simulates techniques that a hacker might use to compromise the software. As with vulnerability testing, penetration testing of software is often done with the assistance of automated tools, which can simulate various types of attacks. As with vulnerability testing tools, there are many penetration testing tools on the market, with varying features and technologies, and which can yield varying results when run against the same software.

d. The term “product security assessments” does not have any specific technical meaning within the industry. It could refer to any type of assessment of the security of a product.

88. Based on the evidence I have reviewed, SolarWinds did all of the things described above during the Relevant Period: It followed an Agile software development methodology, and it incorporated vulnerability testing, regression testing, penetration testing, and product security assessments into its software development lifecycle.

89. Multiple witnesses testified that SolarWinds followed an Agile software development methodology. For example, Steven Colquitt, a Director within Engineering at SolarWinds, testified:

Q. Does SolarWinds use a[n] Agile methodology?

A. Yes, we do.

Q. And can you explain what an Agile methodology involves?

A. So as opposed to a more linear process where you would first do one thing and then do the second thing in a very Waterfall process, we work as a team and iterate in time blocks so that at the end of each time block everything has been done, testing, development testing, security, all of it to a point where you could potentially

release the software at that time. And then that is an iterative approach across a release cycle.¹⁰⁴

90. I have also reviewed documentation from SolarWinds’ software development lifecycle, which reflects an Agile methodology that incorporated security testing consistent with what the Security Statement describes. As Mr. Colquitt testified, SolarWinds’ guidance for its software engineers was contained in a project-management platform, called “Confluence.”¹⁰⁵ I have reviewed various guidance documents from Confluence that indicate SolarWinds followed an Agile development process.¹⁰⁶ In particular, I have reviewed a document titled “Security Testing Process,” created in 2016 and last updated on June 22, 2018, focused on how security testing was integrated into the process.¹⁰⁷ The document explains that there were “two main components of security tests” that were part of SolarWinds’ “agile” software development process:

- “In-sprint” security tests that would be conducted within each “sprint” during the Development phase of the software development lifecycle; and
- “Official” security tests, using “several specialized tools,” which were planned during the Planning phase and executed during the Regression phase.¹⁰⁸

¹⁰⁴ S. Colquitt Dep. Tr. at 25:21-26:8; *see also* J. Kim Dep. Tr. at 119:12-22 (“Q. Did SolarWinds use Agile development methodology? A. Yes. ... Q. Okay. And what is an Agile—what is Agile development methodology? A. Agile development methodology is a software practice where you’re trying to get the value that you’re creating from your products to the hands of your end users as quickly and safely and robustly as possible.”).

¹⁰⁵ S. Colquitt Dep. Tr. at 136:9-18 (“[Q.] If someone said to me, Show me that defined methodology [for developing secure software], what would you show them? A. I would take them to our Confluence documentation platform in the engineering space ...”).

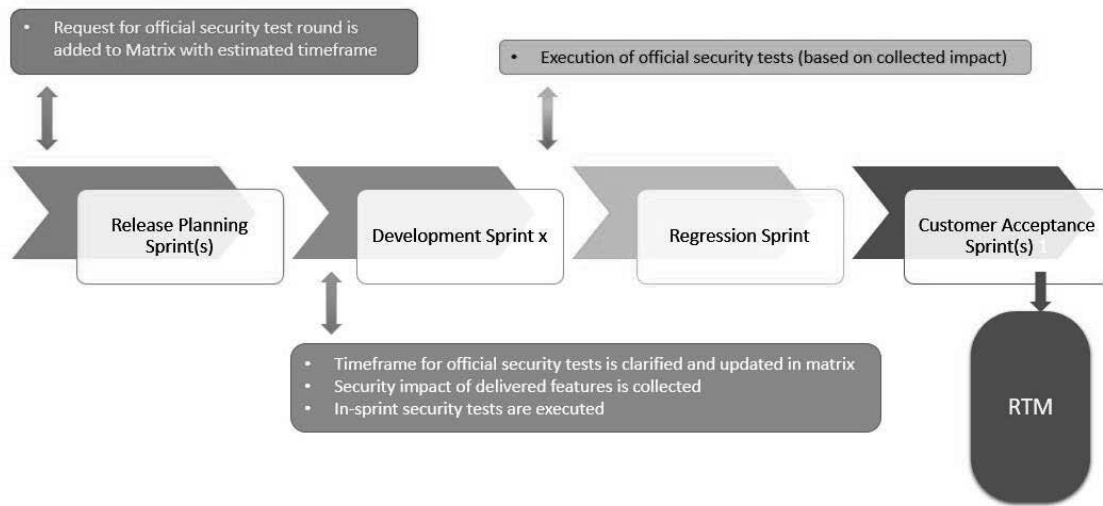
¹⁰⁶ *See, e.g.*, SW-SEC-SDNY_00184277 at -298-302 (document from 2015 titled “SolarWinds Agile Process” providing an overview of the process, including testing done during each sprint); SW-SEC-SDNY_00184276, at slides 7-9 (slide deck from 2015 explaining basics of Agile process, including the bug “scrub” done during each sprint).

¹⁰⁷ SW-SEC-SDNY_00054997 at -997.

¹⁰⁸ *Id.*

The guidance includes a flow chart reflecting the overall process¹⁰⁹:

Release life-cycle from security point of view



91. This guidance reflects an Agile software methodology, with development being done in sprints. It also reflects security considerations being incorporated into each phase of the development lifecycle, as opposed to occurring only at the end—consistent, again, with the Agile methodology and also the Security Statement.

92. I have also reviewed a “Release Checklist” SolarWinds made available on Confluence for engineers to follow as they progressed through the different phases of the software development lifecycle.¹¹⁰ The Release Checklists contain checklist items relating to the “official” security testing described in the above “Security Testing Process” guidance, including:

- during the Planning phase, an entry for “Schedule Security Testing,” which involved selecting an approximate date for “official security testing” by booking it in “Matrix” (a scheduling system) and “start[ing] discussions with Security team if you need any assistance or guidance”¹¹¹

¹⁰⁹ *Id.*

¹¹⁰ See, e.g., SW-SEC00490737 at -737 (“The goal of Release Checklist is to provide a guideline to teams and their stakeholders about activities that happen during a release.”).

¹¹¹ See, e.g., SW-SEC-SDNY_00055081 (“Phase 1 – Planning” checklist).

- during the Development phase, an entry for “Adjust and clarify dates for security tests” in order to “book resources” (i.e., the time of the Security team that would be needed to help run and analyze the security tests)¹¹²
- during the Regression phase, an entry for “Security testing,” where engineers would “[p]lan and execute security testing using Burp Suite [penetration testing software] and other tools”¹¹³

93. I have reviewed samples of over 40 Release Checklists that I received, which were completed by SolarWinds engineers during the development of various products within the Relevant Period, with entries for these tasks being marked completed.¹¹⁴ Below is an example from October 2018, showing the “Security testing” entry in the Regression phase being marked completed¹¹⁵:

Phase 3 - Regression(Hellboy)



Owned by Petr Melichar

Last updated: Oct 29, 2018 by Erik Dresto (Deactivated) • 2 min read • 2 people viewed • Content Report • Legacy editor

Status	What's need to be done	Who	Description
NOT STARTED	Start VPATs Process	PM/PMM	Ensure we get the Voluntary Product Accessibility Template (VPAT) process started as this takes about a month to complete. See page for template.
DONE	Execute integration testing and update Matrix	PO	Execute integration testing for the release, follow the process integration testing. Accept and approve compatibilities and constraints in Matrix once finished.
DONE	Security testing	EM	Plan and execute security testing using Burp Suite and other tools.
DONE	Demo testing	PO	Execute tests for isDemo flag, deliver RC bits to Demo team, cooperate with Demo team
DONE	Stability long-run test, multi-user load test	EM	Perform stability long-run tests inc. multi-user testing

I have also reviewed samples from over 150 JIRA tickets from the Relevant Period with “Security Test” in the title, which reflect security tests that had been scheduled in “Matrix,” as required by

¹¹² See, e.g., SW-SEC-SDNY_00055288 (“Phase 2 – Development” checklist).

¹¹³ See, e.g., SW-SEC-SDNY_00055285 (“Phase 3 – Regression” checklist).

¹¹⁴ See, e.g., SW-SEC-SDNY_00115451; SW-SEC-SDNY_00115457; SW-SEC-SDNY_00115462; SW-SEC-SDNY_00115468; SW-SEC-SDNY_00115471; SW-SEC-SDNY_00115474; SW-SEC-SDNY_00115477; SW-SEC-SDNY_00115478; SW-SEC-SDNY_00115554; SW-SEC-SDNY_00055111; SW-SEC-SDNY_00055271; SW-SEC-SDNY_00055285; SW-SEC-SDNY_00055109; SW-SEC-SDNY_00055269; SW-SEC-SDNY_00055288; SW-SEC-SDNY_00055081; SW-SEC-SDNY_00055107; SW-SEC-SDNY_00055257; SW-SEC-SDNY_00055282; SW-SEC-SDNY_00055266. The entire set I received is contained at: SW-SEC-SDNY_00115446–SW-SEC-SDNY_00115555.

¹¹⁵ SW-SEC-SDNY_00055010.

the Release Checklist.¹¹⁶ (JIRA is a work-tracking system commonly used by technology companies, which was used by SolarWinds.)

94. The most significant artifacts I have reviewed from SolarWinds' software development process, however, are "Final Security Reviews" or "FSRs" that engineering teams were required to prepare at the last phase of the process, prior to release. As Mr. Colquitt testified, this was a new form of documentation SolarWinds rolled out in early 2018, which engineering teams gradually adopted over the ensuing months.¹¹⁷ The FSRs were designed to pull together in one place various artifacts of security testing that were done in connection with a software release across different phases of the development process.¹¹⁸ The FSRs included sections for engineers to post links to tickets ("stories") in JIRA concerning security issues found and addressed through security testing, as well as places to post summaries of or links to the results of vulnerability scans and penetration tests.¹¹⁹

95. I have reviewed a sample from approximately 100 FSRs I received from the Relevant Period, which I understand from Defendants' counsel were retrieved from SolarWinds' Confluence platform, evidencing that these documents were regularly generated as part of SolarWinds' software development process.¹²⁰ From reviewing randomly selected samples of

¹¹⁶ See, e.g., SW-SEC-SDNY_00115117; SW-SEC-SDNY_00115133; SW-SEC-SDNY_00115138; SW-SEC-SDNY_00115220; SW-SEC-SDNY_00115249; SW-SEC-SDNY_00115267; SW-SEC-SDNY_00115312; SW-SEC-SDNY_00115320. The entire set I received is contained at: SW-SEC-SDNY_00115111–SW-SEC-SDNY_115398.

¹¹⁷ S. Colquitt Dep. Tr. at 78:23-79:2, 104:12-105:19 ("[A]t the beginning of 2018 we had updated the release checklist with a requirement to have a final security review.").

¹¹⁸ *Id.* at 77:19-22 ("The final security review is bringing all of the artifacts and results and assessments of our testing together into a central form that's then reviewed by stakeholders.").

¹¹⁹ See, e.g., SW-SEC-SDNY_00069526 at -527 (showing, e.g., "JIRA Board Stories Reviewed").

¹²⁰ See, e.g., SW-SEC-SDNY_00055119; SW-SEC-SDNY_00055163; SW-SEC-SDNY_00055154; SW-SEC-SDNY_00055131; SW-SEC-SDNY_00055310; SW-SEC-SDNY_00115102; SW-SEC-SDNY_00074874; SW-SEC-SDNY_00072815; SW-SEC-SDNY_00069526; SW-SEC-SDNY_00089995; SW-SEC-SDNY_00069825; SW-SEC-SDNY_00055006; SW-SEC-SDNY_00055028; SW-SEC-SDNY_00055225. The entire set I received is contained at: SW-SEC-SDNY_00069496–SW-SEC-SDNY_00115110. Note that some of the FSRs contain broken links to queries in JIRA that would otherwise pull JIRA tickets relating to the FSR into the document. (This appears as an error message stating "Unable to locate Jira server for this macro. It may be due to Application Link configuration.")

these FSRs, I have observed they contain numerous artifacts of security testing. These include, among other things, links to design reviews done by the Architecture Team, links to JIRA tickets concerning resolution of potential security vulnerabilities that had been identified during development, reports or summaries of findings from “Checkmarx” or “Whitesource,” which are vulnerability scanning tools, and summaries of or references to reports from “Burp,” i.e., Burpsuite, which is a penetration testing tool.¹²¹

96. I have also reviewed samples of the underlying artifacts referenced in these FSRs. These include samples from approximately 500 Checkmarx reports and more than 100 Burpsuite reports generated during the Relevant Period, reflecting the results of vulnerability scans and penetration tests that were conducted during the software development process.¹²² I have also reviewed samples out of hundreds of JIRA tickets I have received that are cross-referenced in the FSRs, which reflect individual security risks that were flagged through testing or analysis of the code and proposed or completed mitigations.¹²³ Additionally, I have reviewed samples out of more than 2,000 JIRA tickets I have received reflecting regression tests that were run during the

I am informed by Defendants’ counsel this error appears because the company migrated to a new JIRA server during the Relevant Period, which broke links to JIRA created prior to the migration. I am also informed by Defendants’ counsel that they made a document production that includes missing tickets. See SW-SEC-SDNY_00191599–SW-SEC-SDNY_00192861.

¹²¹ See *id.*

¹²² See, e.g., Checkmarx scans, SW-SEC-SDNY_00177999; SW-SEC-SDNY_00180217; SW-SEC-SDNY_00182941; SW-SEC-SDNY_00178368; SW-SEC-SDNY_00178503; SW-SEC-SDNY_00179088; SW-SEC-SDNY_00175512; SW-SEC-SDNY_00175926; SW-SEC-SDNY_00176568; SW-SEC-SDNY_00176936; and BurpSuite reports, SW-SEC-SDNY_00159807; SW-SEC-SDNY_00138546; SW-SEC-SDNY_00125488; SW-SEC-SDNY_00126005; SW-SEC-SDNY_00078650; SW-SEC-SDNY_00142863; SW-SEC-SDNY_00126057; SW-SEC-SDNY_00138781. The entire set of Checkmarx scans I received is contained at: SW-SEC-SDNY_00175331–SW-SEC-SDNY_00183311. The entire set of BurpSuite reports I received is contained at: SW-SEC-SDNY_00115782–SW-SEC-SDNY_00175330.

¹²³ See SW-SEC-SDNY_00191599; SW-SEC-SDNY_00191606; SW-SEC-SDNY_00191618; SW-SEC-SDNY_00191853; SW-SEC-SDNY_00191832; SW-SEC-SDNY_00192020; SW-SEC-SDNY_00192221; SW-SEC-SDNY_00192346; SW-SEC-SDNY_00192747; SW-SEC-SDNY_00192845. The entire set I received is contained at: SW-SEC-SDNY_00191599–SW-SEC-SDNY_00192861.

Relevant Period as part of the software development process.¹²⁴

97. The collective evidence I have reviewed easily allows me to conclude that the representations in the Security Statement concerning SolarWinds' software development lifecycle were accurate. SolarWinds followed an Agile software development methodology, and there are large volumes of evidence reflecting that it incorporated security testing into the various phases of the development process. Notably, the level of documentation of these practices—in particular the FSRs—goes beyond what I would expect to see. Software companies widely vary in terms of the level of documentation they generate around their security-testing activities, and engineers are not always focused on formally documenting their work (as opposed to working directly on the code). The available documentation in my view therefore provides particularly strong evidence that security testing was a mandated and regularly conducted part of SolarWinds' software development lifecycle.

VI. THE GRAFF REPORT IS FUNDAMENTALLY FLAWED AND DOES NOTHING TO CHANGE MY CONCLUSIONS

98. In conjunction with reaching my affirmative opinions about SolarWinds' cybersecurity controls, I was provided with and reviewed the Graff Report. My analysis of the Graff Report included a review of Mr. Graff's opinions and the methodology through which he arrived at them. Although I had full confidence in my opinions after conducting my affirmative assessment (following the process outlined above), in reviewing the Graff Report I considered whether I had missed any important documents or considerations. For the reasons stated below, nothing in the Graff Report changes any of my opinions. If anything, the deficiencies in Mr.

¹²⁴ See SW-SEC-SDNY_00184530; SW-SEC-SDNY_00185504; SW-SEC-SDNY_00185769; SW-SEC-SDNY_00185815; SW-SEC-SDNY_00185849; SW-SEC-SDNY_00186209; SW-SEC-SDNY_00186303; SW-SEC-SDNY_00186410; SW-SEC-SDNY_00187520. The entire set I received is contained at: SW-SEC-SDNY_00184391–SW-SEC-SDNY_00189216.

Graff's methodology, and the documents and events cited in support of his opinions, make me even more confident in my conclusions.

A. Mr. Graff Does Not Follow Any Valid Methodology

99. As discussed above, it is my opinion that SolarWinds adhered to the representations in the Security Statement throughout the relevant period. I arrived at that opinion after considering—among other things—large volumes of artifacts demonstrating the design and day-to-day implementation of the practices outlined in the Security Statement, as well as the sworn testimony of SolarWinds employees responsible for these controls, including employees with personal knowledge of the documents on which Mr. Graff relies. Occasional wrinkles or lapses in implementing these controls are expected and do not undermine the broad representations in the Security Statement—which, in my opinion, should not and would not be interpreted as a guarantees of perfection.

100. Mr. Graff's contrary opinion is “that several of the cybersecurity issues raised in [SolarWinds] internal documents indicate that SolarWinds failed to consistently apply the cybersecurity practices described in the Security Statement.”¹²⁵ In support of that opinion, Mr. Graff relies on a limited number of supposed “discrepancies” or “nonconformities” with the Security Statement's representations regarding user access controls, password complexity requirements, and software development. My understanding is that Mr. Graff located this small set of documents (which he recycles throughout the different sections of his report) among the more than 120,000 documents produced to the SEC in this case. I disagree with Mr. Graff's interpretation of these limited, discrete events—both individually and in aggregate. They simply do not support the broad conclusions he draws from them.

¹²⁵ Graff Report ¶ 48.

101. Generally speaking, there are several recurring problems with Mr. Graff's methodology. *First*, the process he follows does not resemble any standard cybersecurity assessment as such assessments are performed in the industry. I have years of experience performing security assessments, and in my opinion, Mr. Graff's approach is not an accepted way to conduct one. Cybersecurity assessments generally do not involve reviewing employees' emails or presentations to management in the first place (let alone stray comments or notations in such documents that lack appropriate context). Standard methodology instead is to examine *direct evidence* of the company's implementation of those controls—in the form of written policies describing the controls and day-to-day documentation generated from the operation of the controls.¹²⁶ As discussed above, the policies and artifacts available show that SolarWinds had processes that were designed and implemented as stated in the Security Statement.¹²⁷ Mr. Graff simply ignores all of that evidence, even though it is the core evidence that would inform a standard cybersecurity assessment.

102. *Second*, as to the documents Mr. Graff relies on instead, he repeatedly takes remarks in them out of context and disregards what witnesses with knowledge about the documents have said about them. This, too, departs from standard practice. To the extent I am doing a cybersecurity assessment and find a comment in a document that raises a concern for me, the appropriate course of action is to ask to communicate with employees knowledgeable about those records to learn more about them, as there is often important context that may not be apparent from the documents themselves. Mr. Graff did none of that. Instead, his analysis consisted of zeroing in on isolated notations in emails, slide presentations, and other documents, and speculating about their meaning, while ignoring the context for them, including the sworn testimony of witnesses

¹²⁶ *Supra* ¶¶ 17-21.

¹²⁷ *Supra* Section V.

who wrote or knew about the notations at issue, which made clear that they do not have the broad meaning that Mr. Graff ascribes to them.

103. *Third*, Mr. Graff is never clear about the standard he is applying. He repeatedly concludes that SolarWinds did not “consistently” adhere to the policies described in the Security Statement. But he does not define what he means by “consistently.” Instead, he simply points to what he characterizes as instances in which these policies were deviated from. Yet at the same time, Mr. Graff repeatedly acknowledges that it is unreasonable to demand perfection as the standard. As he states, “no organization has perfect cybersecurity and [] any organization diligently assessing its cybersecurity will uncover, from time to time, some issues needing to be addressed.”¹²⁸ Indeed, if a cybersecurity program at a company the size of SolarWinds—which had approximately 3,000 employees during the Relevant Period¹²⁹—*was not* regularly identifying and fixing these sorts of issues, that would suggest to me that there was a problem with the cybersecurity program. Accordingly, if all Mr. Graff means in saying that the policies articulated in the Security Statement were not implemented “consistently” is that they were not implemented *perfectly*—i.e., that there were lapses or discrepancies from time to time—that is to be expected. That conclusion would not imply that the policies stated in the Security Statement were “false” or “misleading,” because anyone in the industry reading it would understand that the policies were not meant to be guarantees of perfection.

104. If, instead, Mr. Graff’s opinion is that SolarWinds *pervasively* failed to implement the policies in the Security Statement—which is what the SEC alleges throughout its Amended

¹²⁸ See, e.g., Graff Report ¶ 101.

¹²⁹ See SolarWinds, Form 10-K, Feb. 25, 2019, <https://investors.solarwinds.com/financials/sec-filings/sec-filings-details/default.aspx?FilingId=13251537>, at 10 (stating the company had 2,738 employees); SolarWinds, Form 10-K, Feb. 24, 2020, <https://investors.solarwinds.com/financials/sec-filings/sec-filings-details/default.aspx?FilingId=13946190>, at 9 (stating that the company had 3,251 employees).

Complaint¹³⁰— then Mr. Graff fails to adequately explain how he can validly extrapolate to this conclusion from the limited information he relies upon. This is a fundamental and, frankly, elementary flaw in Mr. Graff’s analysis. He asserts that the purported lapses he identifies “suggest” or are “indicative” of “systemic issues” at SolarWinds,¹³¹ but he nowhere even attempts to measure these purported lapses against some kind of denominator in a way that would show they were pervasive. For example, he identifies one non-compliant password that existed on one system during the Relevant Period, but he ignores that this would have been one of thousands of passwords used across thousands of systems at SolarWinds, and he makes no effort to show how the one example he cites can be assumed to be representative of SolarWinds’ password practices more broadly. Nor does Mr. Graff identify any benchmark for an expected or acceptable error rate against which to judge the implementation of SolarWinds’ controls—even though he acknowledges repeatedly that errors and lapses occur in any cybersecurity program.¹³²

105. Notably, Mr. Graff had access to the same testimony and types of documents as I have had, which, as I described above, demonstrate how the policies stated in the Security Statement were applied on a day-to-day basis. *That* evidence reflects SolarWinds’ “systemic” practices. Yet Mr. Graff seems to have deliberately excluded such evidence from his review. Surprisingly, Mr. Graff himself essentially acknowledges this, stating that “[e]ven if [he] had

¹³⁰ See Am. Compl. ¶ 2 (alleging that SolarWinds had “long-standing, pervasive, systemic, and material cybersecurity deficiencies” and that it “systemically failed to follow many of the industry-standard cybersecurity practices to which the Company claimed to adhere”); *id.* ¶ 11 (alleging “pervasive cybersecurity problems”); *id.* ¶ 73 (alleging “failures so pervasive in critical areas that they represented systemic problems, and programmatic failures across wide swaths of SolarWinds or even the entire Company”); *id.* ¶ 102 (alleging that “there were many critical areas or controls where SolarWinds did not have a program or practice in place” and that there were “systemic, organizational-level failures to employ adequate policies and procedures”); *id.* ¶ 115 (alleging that SolarWinds “pervasively failed to develop software in a secure development lifecycle” (capitalization altered)); *id.* ¶ 154 (alleging a “systemic” failure to conduct network monitoring); *id.* ¶ 182 (alleging SolarWinds “pervasively granted employees unnecessary ‘admin’ rights”); *id.* ¶ 226 (alleging that SolarWinds had “pervasive cybersecurity issues” that were “part of a systemic cybersecurity problem”).

¹³¹ Graff Report ¶¶ 78, 91, 92, 157, 158.

¹³² *Id.* ¶ 101.

found a large number of additional internal documents describing SolarWinds adhering to industry norms at times, these would not have changed my opinions.”¹³³ Disregarding artifacts showing “SolarWinds adhering to industry norms,” particularly large numbers of them, is incompatible with any reasonable assessment methodology that I am familiar with. And as a matter of basic logic, excluding such evidence from review makes it impossible to draw any reliable conclusion about what “consistently” did or did not happen.

106. As a substitute for determining the pervasiveness with which SolarWinds identified lapses in its cybersecurity controls, Mr. Graff opines that even though the lapses he identifies may have been small in number, they were supposedly of such serious “magnitude” that they are “indicative of systemic issues.”¹³⁴ That conclusion does not follow either. Even if the issues he identifies were major departures from SolarWinds’ stated practices (and, as explained below, they were not), the magnitude of an issue has nothing to do with how frequent it is. Aaron Judge made an error in this year’s World Series that cost the Yankees the final game; that was a momentous mistake, but it hardly means he is a bad baseball player. (In fact, it was his first error of the year.)¹³⁵ Mr. Graff simply does not explain what basis he has to assume that the few specific events he focuses on represent SolarWinds’ general practices with respect to the policies at issue, or to conclude from these events that SolarWinds pervasively failed to implement those policies.

107. Even setting aside these basic methodological and analytical flaws in Mr. Graff’s conclusions, I disagree with his characterizations of the examples he cites to support his opinions regarding SolarWinds’ user access controls, password controls, and implementation of secure

¹³³ *Id.* ¶ 46.

¹³⁴ *See, e.g., id.* ¶ 77 (“The fact that such major events slipped through the cracks is indicative of systemic issues.”); *id.* ¶ 101 (opining that the examples Mr. Graff cited “do not constitute the kind of routine minor problems” he would expect).

¹³⁵ *Dodgers Clinch Title After Yankees Blow 5-Run Lead*, Associated Press (Oct. 16, 2024), <https://apnews.com/article/world-series-yankees-errors-ff3ca215e6064c1983e4cce4f41a97e0>.

software development practices. They are not events of significant magnitude. They are the sorts of issues that routinely come up at any cybersecurity program of significant size. They reflect exactly what good cybersecurity programs *do* on a day-to-day basis: respond to incidents, spot risks requiring mitigation, and identify opportunities for improvement.

108. At bottom, none of the issues cited by Mr. Graff change my opinions because they simply distract from the only relevant question: whether SolarWinds had processes in place that were consistent with its representations in the Security Statement. Based on the artifacts and testimony I have reviewed, it clearly did.

B. Mr. Graff Misinterprets What It Means to Follow the NIST Framework

109. Mr. Graff seems to take a different position from the SEC with respect to the meaning of the Security Statement’s representation that SolarWinds followed the NIST CSF. The SEC has alleged that the representation was untrue because of purported “low scores” SolarWinds gave itself in NIST CSF assessments,¹³⁶ whereas Mr. Graff argues that the representation is either “too vague” to evaluate or that it was untrue because SolarWinds supposedly failed to adhere to unspecified “best practices.”¹³⁷ In my opinion, both the SEC and Mr. Graff misinterpret what it means to follow the NIST CSF.

110. In its Amended Complaint, the SEC takes the position that SolarWinds cannot be considered to have followed the NIST CSF because it supposedly rated itself poorly in certain categories in conducting self-evaluations under the framework.¹³⁸ This position fundamentally misunderstands the nature of the NIST CSF. As explained above, the NIST CSF does not set any

¹³⁶ Am. Compl. ¶¶ 88, 91.

¹³⁷ Graff Report ¶ 21.

¹³⁸ Am. Compl. ¶¶ 76 (“In claiming to ‘follow’ the NIST Cybersecurity Framework, Brown and SolarWinds made a materially false and misleading statement or omission by not revealing how poorly SolarWinds fared on multiple internal assessments using the Framework ...”); *id.* ¶ 109 (“Claiming to ‘follow’ the NIST Cybersecurity Framework during the Relevant Period, without disclosing how poorly SolarWinds assessed itself ... was misleading.”).

substantive standard or minimum scores that a company must meet.¹³⁹ It is not a “test” that an organization “passes” or “fails.” It is a governance framework that an organization can use to evaluate how sophisticated its various cybersecurity controls are, in order to determine where to focus its improvement efforts. That is what following the NIST CSF means, and that is exactly what SolarWinds did. What scores the company gave itself in any particular categories is irrelevant.

111. The SEC in the Amended Complaint also conflates the NIST CSF with NIST Special Publication 800-53 (“NIST SP 800-53”).¹⁴⁰ Unlike the NIST CSF, NIST SP 800-53 *is* a standard that sets forth specific cybersecurity controls that must be achieved in order to meet it. There is a relationship between the two documents: NIST CSF lists NIST SP 800-53 among various “Informative References” that an organization can consult in evaluating itself for purposes of a NIST CSF assessment.¹⁴¹ NIST guidance makes clear, however, in the context of conducting a NIST CSF assessment, Informative References such as NIST SP 800-53 “should not be viewed as a checklist that must be completed to implement the subcategory outcome. Organizations can use some, none, or all the Informative References to inform the activities they undertake to achieve the outcome described by the Subcategory.”¹⁴² In other words, organizations conducting a NIST CSF assessment can choose to use NIST SP 800-53, or parts of it, as a benchmark *if they want*; but following the NIST Framework does not *require* meeting the NIST SP 800-53 standard—or any other particular cybersecurity standard.

112. For his part, Mr. Graff seems to have a different understanding of this

¹³⁹ *Supra* Section V.B.

¹⁴⁰ Am. Compl. ¶¶ 92-102.

¹⁴¹ *Informative References: What Are They, and How Are They Used?*, NIST (Apr. 12, 2018), <https://www.nist.gov/cyberframework/online-learning/informative-references>.

¹⁴² *Id.*

representation from the SEC, as he does not try to claim that the representation was false due to any supposedly “low scores.” Instead, at least initially, he asserts that the representation is “too vague ... to evaluate.”¹⁴³ This position, too, is incorrect. It is true, as Mr. Graff points out, that the NIST CSF “does not prescribe” specific controls which “the organization must adopt.”¹⁴⁴ (That is exactly why the SEC’s position is misguided.) But that does not mean the NIST CSF is devoid of content. Again, when companies say that they follow the NIST CSF, they typically mean that they follow a structured process along the lines the NIST CSF lays out for regularly evaluating their cybersecurity program and continuing to improve it over time. That is a component of good cybersecurity governance that companies may wish to communicate they have in place. Indeed, it is common for companies to mention their use of the NIST CSF in the cybersecurity governance sections of their annual investor filings (a new section of 10-K filings created through an SEC rulemaking last year). For example, the Form 10-K for General Motors Financial Company for FY 2023 states:

We design and assess our program based on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). This does not imply that we meet any particular technical standards, specifications, or requirements, but rather that we use the NIST CSF as a guide to help us identify, assess, and manage cybersecurity risks relevant to our business.¹⁴⁵

I understand the representation about the NIST CSF in the Security Statement in the same way:

¹⁴³ Graff Report ¶ 21.

¹⁴⁴ *Id.*

¹⁴⁵ See General Motors Financial Company, Inc., Form 10-K, Jan. 30, 2024, <https://www.sec.gov/Archives/edgar/data/804269/000080426924000004/acf-20231231.htm>, Item 1.C; see also, e.g., Digital Realty Trust, Inc., Form 10-K, Feb. 23, 2024, <https://www.sec.gov/Archives/edgar/data/1494877/000155837024001575/dlr-20231231x10k.htm>, Item 1.C (“We utilize the United States National Institute of Standards and Technology, Cybersecurity Framework (NIST CSF) in considering the design and in assessing our processes. This does not imply that we meet any particular technical standards, specifications, or requirements, only that we use the NIST CSF as a guide to help us identify, assess, and manage cybersecurity risks relevant to our business.”); SkyWest, Inc., Form 10-K, Feb. 15, 2024, <https://www.sec.gov/Archives/edgar/data/793733/000155837024001237/skyw-20231231x10k.htm>, Item 1.C (“[W]e have aligned our processes with the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and assess our cybersecurity maturity against the NIST CSF’s core functions; however, this does not imply that we meet any particular technical standards, specifications or requirements, only that we use the NIST CSF as a guide to help us identify, assess and manage cybersecurity risks relevant to our business.”).

not as a statement that SolarWinds met any particular technical standards, but rather as a statement about its cybersecurity governance—i.e., a statement that it regularly self-assessed its cybersecurity posture and used the NIST CSF as a guide in doing so.

113. Confusingly, after concluding that the statement that SolarWinds followed the NIST CSF is “too vague ... to evaluate” and “not verifiable,” Mr. Graff proceeds to ascribe his own meaning to the statement, asserting that it “indicates that SolarWinds routinely followed cybersecurity norms and best practices,” which he argues was false.¹⁴⁶ However, the statement says nothing about “cybersecurity norms and best practices”¹⁴⁷—which itself is a vague phrase that Mr. Graff does not define. And there is no reason why a statement about following the NIST Framework must be read as if it were a commitment to implementing certain “norms” or “best practices.”¹⁴⁸ Apart from the self-evaluation process it sets forth, the NIST CSF does not mandate any specific “norms” or “best practices” that all companies are supposed to follow. To the contrary, the NIST CSF expressly disavows a “one-size-fits-all approach” and recognizes that companies can choose how rigorous and sophisticated their controls should be, based on their individual circumstances and risk appetites.¹⁴⁹ Mr. Graff himself seems to recognize this in acknowledging that the NIST CSF “is not literally a standard” and does not “prescribe which ... controls [an] organization must adopt.”¹⁵⁰ Mr. Graff therefore has no basis to treat the Security Statement’s reference to NIST CSF as a standard requiring a company to meet some (undefined) set of “cybersecurity norms and best practices.”

¹⁴⁶ Graff Report ¶ 21.

¹⁴⁷ See SW-SEC00466129 at -129.

¹⁴⁸ See *id.*

¹⁴⁹ *Supra* ¶¶ 32-38.

¹⁵⁰ Graff Report ¶ 21.

C. Mr. Graff Does Not Show Any Systemic Failure to Implement Role-Based Access Controls

114. In my opinion, nothing in Mr. Graff's report shows that SolarWinds failed to implement role-based access controls in the manner described in the Security Statement.

115. As an initial matter, Mr. Graff makes little effort to address the most important evidence of SolarWinds' role-based access controls—the testimony and artifacts concerning how users were provisioned with access at SolarWinds. As I described above, if an outside expert were hired to conduct a security assessment of SolarWinds and were trying to determine how SolarWinds provisioned employees with access rights, the methodology they would typically follow would be to interview witnesses knowledgeable about those processes and then to collect and review sample evidence of those processes. In this litigation, there are not merely interviews but sworn testimony from multiple witnesses describing SolarWinds' practices around role-based access controls—including the SARF process, user access reviews, and alerts sent to InfoSec whenever someone was granted administrative access—and how all of these processes and procedures were designed to ensure users were given access to only those systems they needed for their roles. Moreover, there is an abundance of artifacts showing that these processes and procedures were actually implemented on a day-to-day basis during the Relevant Period.

116. Mr. Graff appears to have largely excluded this evidence from his review or, for reasons he did not explain, found it irrelevant. Instead, Mr. Graff's methodology involves making unwarranted inferences from a small number of documents. There are essentially two types of unwarranted inferences Mr. Graff makes: First, he takes isolated events or issues and makes hasty generalizations from them, in order to conclude that SolarWinds broadly failed to implement role-based access controls or the principle of least privilege, when that is simply not what the cited documents show. Second, he takes vague remarks in various documents out of context and treats them as admissions of systemic failures, when that interpretation is not supported by the evidence

and is specifically contradicted by the people who actually wrote the remarks.

117. I do not attempt to address each and every one of these unwarranted inferences that Mr. Graff makes, as they quickly grow repetitive. However, below I analyze the main examples Mr. Graff relies upon, which illustrate the flaws that run throughout Mr. Graff's methodology.

1. Mr. Graff's Unwarranted Extrapolation from Isolated Events

118. *Help-desk Ticket About Onboarding a "Temp" Employee.* One example of the hasty generalizations Mr. Graff makes is the single instance where Mr. Graff actually discusses the SARF process. Mr. Graff mentions the SARF process only briefly, in challenging the Security Statement's representation that "[p]rocesses and procedures are in place to address employees who are voluntarily or involuntarily terminated."¹⁵¹ Specifically, Mr. Graff cites a help-desk ticket implementing a SARF form for a "temp" employee that was being onboarded. He states that the ticket reflects an "ad-hoc process," because it includes a chat in which a help-desk employee notes that there was no date listed on the SARF form indicating when the temp would "finish," and someone tells the employee in response to make it for "1 year."¹⁵² From this sliver of evidence, Mr. Graff concludes that the SARF process was "an ad-hoc process" and that this shows that SolarWinds did not "consistently implement" processes and procedures to deprovision access for terminated employees.¹⁵³

119. There are several things wrong with this very cursory reasoning. First, it is not even clear from the chat that the "1 year" time period was incorrect; the person who specified the time period may have gotten it from the temp's manager, or that period may have been a standard employment period for a temp.¹⁵⁴ Moreover, even if the one-year end date was not correct, it does

¹⁵¹ Graff Report ¶¶ 98-99.

¹⁵² *Id.* ¶ 98 & n.182 (citing SW-SEC-SDNY_00050922 at -922).

¹⁵³ *Id.* ¶¶ 98-99.

¹⁵⁴ SW-SEC-SDNY_00050922 ("Was there a date given to when the temp will finish? ... No, none.").

not imply that the temp’s access would not have been terminated if the individual left the company earlier than a year. To the extent Mr. Graff makes that assumption, he ignores the testimony and evidence reflecting that a *separate* SARF would be submitted upon an employee’s termination, which would have caused the temp’s access to have been deprovisioned regardless of any end date listed on their original SARF.¹⁵⁵

120. But more fundamentally, by focusing on this one particular help-desk ticket, Mr. Graff misses the forest for the trees. What this and many other help-desk tickets and corresponding SARF forms show is that SolarWinds had processes and procedures in place for provisioning employees with access to resources based on what they needed for their role. Even if some forms might not be filled out entirely correctly or if errors were sometimes made in the process, the fact remains that processes and procedures were in place. Indeed, user access reviews were included as part of those processes and procedures, which were designed to catch provisioning errors—including if an employee’s access was accidentally not deactivated after they were terminated.¹⁵⁶ Mr. Graff provides no evidence that SolarWinds’ processes and procedures for addressing terminated employees were routinely disregarded or misapplied. He does not even seem to conclude that; instead he vaguely states that processes and procedures were not “consistently” applied.¹⁵⁷ If all Mr. Graff means is that there were occasional errors in implementing those processes and procedures, then that does not contradict the Security Statement, which merely said that processes and procedures were “in place.” It did not say that they were perfectly implemented; nor would anyone in the industry reading the Security Statement expect that, as Mr. Graff himself

¹⁵⁵ See *supra* ¶ 50.

¹⁵⁶ See *supra* ¶ 53 & n.50.

¹⁵⁷ Graff Report ¶ 99.

repeatedly seems to acknowledge.¹⁵⁸

121. *Developer Access to Billing Data for Test Purposes.* Mr. Graff’s other hasty generalizations do not even concern the SARF process, but instead concern one-off issues with marginal if any relevance to SolarWinds’ procedures for provisioning users with access rights. For example, Mr. Graff describes a situation in which he asserts “certain developers had unnecessary access to a dataset.”¹⁵⁹ I have reviewed the email chain he cites, and that is not even what it reflects; but in any event it certainly does not reflect any systemic failure to implement role-based access controls.

122. What the cited email chain reflects is that, in November 2019, certain software developers were working on “improving [the] billing system” used by SolarWinds’ Finance Department.¹⁶⁰ The developers needed access to billing data in “production”—i.e., data in the live billing system that finance employees were using on SolarWinds’ corporate network—in order to test the improvements they were developing.¹⁶¹ In order to access that data, the developers had apparently borrowed the credentials of a different SolarWinds employee with “SuperUser” access, which was the type of access needed to pull the relevant data.¹⁶² Borrowing another user’s

¹⁵⁸ *Id.* ¶¶ 25, 50, 76, 79, 101. Likewise, Mr. Graff cites testimony from Rani Johnson, SolarWinds’ Chief Information Officer during the Relevant Period, stating that there were a “few instances” where a terminated employee’s access was not cut off within a “day period” of their departure, and that one user access review identified 18 users whose accounts had not been deactivated even though they were “inactive contractors and/or vendors.” *Id.* ¶ 97. The fact that SolarWinds occasionally identified, over a multi-year period, a small number of employees or contractors—out of thousands who worked for the company—whose access may not have been promptly revoked upon termination does not imply that it lacked processes and procedures for deprovisioning access of terminated personnel. Indeed, the practice of doing regular user access reviews was itself such a procedure and was designed to catch any such errors.

¹⁵⁹ *Id.* ¶ 79.

¹⁶⁰ SW-SEC00254254 at -258.

¹⁶¹ *Id.* at -265 (explaining that “we were developing billing using production services since the beginning as only production has data to test billing”); *id.* at -264 (explaining it would require engineering effort to obtain “enough test data” without “going to production” for it); *id.* at -260 (explaining that the issue was “how best to secure access to production data in order to improve our billing systems”).

¹⁶² *Id.* at -265 (explaining that the developers were “using a shared login currently of a different SolarWinds employee,” which “needs to stop”); *id.* at -255 (explaining that the developers were using “shared logins with Superuser access to Production Backup data in order to pull data for billing” through two different APIs).

credentials was flagged as a security violation, leading the developers to request SuperUser access for themselves—consistent with the procedures I described earlier, requiring any grant of non-standard access rights to be requested and approved.¹⁶³

123. The request was evaluated by the InfoSec team, including Tim Brown. It was recognized that the ideal solution was to create a copy of the billing system that the engineers could test separately from the live version, but that option was not technically feasible in any foreseeable timeframe.¹⁶⁴ As a result, the developers needed access to the live data, and a SuperUser account was required in order to pull the data.¹⁶⁵ However, a SuperUser account came with both “read” and “write” access—i.e., the ability to both view and modify the data—whereas the developers only needed to read the data.¹⁶⁶ There was not an existing “read-only” level of privilege that could be provided for the systems in question; and creating one would require engineering work that would take time. The solution arrived at was to (a) give the developers SuperUser accounts for the time being so that they could continue working on the project and (b) eventually create a special “read-only” level of access that the developers could use, once the relevant engineering resources freed up to do that work.¹⁶⁷ Mr. Brown documented the decision in a Risk Acceptance Form, which deemed the risk from granting the developers SuperUser access to be “Low” and outweighed by the benefit of allowing them to complete the work they were doing, which was

¹⁶³ See *id.* at -258 (“This is a request we will always challenge as ... it is unusual to give this level of access to developers on production systems.”).

¹⁶⁴ See *id.* at -258 (“I would love to develop only on staging, but our billing system is complicated and our staging doesn’t reflect production customer tree and also staging doesn’t have all billing cases which we have in production. We’ve been trying to move [the developers] to staging for a while, but it’s hard to resolve items above.”).

¹⁶⁵ See *id.* at -254-255 (“Currently BizApps is blocked with moving forward ... because they need access to one more API to pull this data from Backup. ... Short-Term Solution: ... BizApps would be granted Superuser access to the new API which would unblock us and we could move forward with our Backup O365 billing project.”).

¹⁶⁶ See *id.* at -263 (explaining that the data at issue was “limited to SuperUser access level” and that “this level has read&write permissions”).

¹⁶⁷ See *id.* at -255 (explaining “Short-Term Solution” and “Long-term Solution”).

considered to be an important billing project.¹⁶⁸

124. Mr. Graff argues that “a problem of this magnitude” implies that “practices were not in place” to ensure that the Security Statement’s representations about role-based access controls “were consistently implemented across the organization.”¹⁶⁹ This hardly follows from the above facts. First of all, this was not a “problem” of significant “magnitude.” The developers needed access to live billing data in order to perform their role, and there was no readily available way to give them that access without providing them with a SuperUser account. While SuperUser access came with “write” access, the only risks from granting that access were the risk that they might accidentally modify the data, or the highly remote risk that they would intentionally modify it. And this was merely *billing* data; it was sensitive from a SOX perspective, because it related to SolarWinds’ financial reporting, but it had nothing to do with the security of SolarWinds’ products.

125. While Mr. Graff strains to portray this and other issues as somehow akin to “not locking the front door” of a house, the analogy is not remotely apt.¹⁷⁰ The situation here would be more analogous to giving a small set of trusted employees access to a file cabinet containing billing records—which they needed to view to do their job—with the risk being that they might spill coffee on the records while reviewing them or, in some farfetched scenario, that they might alter them for malicious purposes. While ideally it would be preferable set up a special room where they were not allowed to bring in coffee or a pen, the risk of simply allowing them to access the file cabinet directly would be low, and it would be reasonable for the business to accept that risk in order to get the work done. That is all that happened here.

¹⁶⁸ See SW-SEC00168780, Row 9 (accepting risk given that “[b]enefits” would be to “[a]llow[] BizApps Dev to continue their development work and not delay a major project” and “[l]evel of [r]isk” was “Low”).

¹⁶⁹ Graff Report ¶ 84.

¹⁷⁰ *Id.* ¶ 104.

126. This incident does not evidence any systemic lack of role-based access controls at SolarWinds. If anything, it further evidences that role-based access controls were in place. The developers at issue did not themselves have the access they sought. They at first improperly borrowed an account of another employee to obtain it; but that was detected as a security violation. When they then went through the proper channels and requested the access in question, the request was evaluated by the InfoSec team, which determined that the access was needed for their role and approved the access, with a plan to limit it further in the long-term. This shows that SolarWinds was attentive to the principle of limiting employee access rights based on what was needed for their role, and that it went through a reasoned process to apply this principle to this special case. If SolarWinds actually lacked role-based access controls, the developers in question would not have even needed to ask to have the privileges at issue added to their accounts (or needed to improperly borrow someone else's account). Their access would have been unlimited to begin with.

127. *MSP Customer Support Staff's Access to MSP Customer Environments*. Mr. Graff also cites a draft slide deck, titled "MSP Support Security Improvement," raising a concern about MSP customer support staff having excessive access to customer environments.¹⁷¹ There are several problems with Mr. Graff's analysis of this issue. As an initial matter, the document he cites is a *draft* document in which most of the slides are either unfinished or entirely blank,¹⁷² and he does not cite any deposition testimony about this slide deck (nor am I aware there was any). So the document is a questionable basis on which to draw any conclusions about anything.

128. In any event, the slide deck appears to have been about merely fine-tuning the access that SolarWinds' MSP customer support representatives had to customer environments.

¹⁷¹ *Id.* ¶ 68 (quoting SW-SEC00631418).

¹⁷² SW-SEC00631418 at -420-422 (containing half-finished and blank slides).

SolarWinds’ MSP business served customers that are themselves MSPs—“managed service providers,” i.e., outsourced IT providers for other business—and sold MSPs software that they used to run their operations. SolarWinds’ MSP customer support representatives needed to be able to access its customers’ environments in order to diagnose problems customers were having using SolarWinds’ software. Such remote access is a common way of addressing customer support issues. The concern raised in the draft slide deck is that customer support representatives did not always need full admin access in performing that role, and there were risks associated with that level of access—as highlighted by a recent incident where data in a customer environment had been accidentally altered by SolarWinds personnel.¹⁷³ So this deck appears to have been proposing various technical changes to limit the scope of the access that support staff had, including the creation of a new read-only type of customer support account separate from an admin account, which would have required engineering work on SolarWinds’ MSP customer support system in order to implement.¹⁷⁴

129. Again, this highly specific issue does not evidence any general lack of role-based access controls at SolarWinds or any general disregard for the principle of least privilege. This was an edge case in which access to MSP customer systems was already limited to a discrete set of employees who needed access to those systems in order to perform their role. SolarWinds was simply considering how to limit their access even further in response to a particular risk being identified. This is, again, not akin to someone leaving the front door open at their house. Rather, it is more like running a housekeeper service in a hotel, in which the housekeepers can access customers’ rooms to do their jobs. The proposal was simply to add an extra layer of security to the arrangement, akin to installing safes where the customers could place their valuables.

¹⁷³ SW-SEC00631418 at -419.

¹⁷⁴ *Id.*

130. As I know from my experience as a CISO at a large organization, this is what a well-functioning cybersecurity program does on a daily basis: It has general processes in place, but is always on the lookout for specific areas where those processes can be improved. People in the industry would understand that in reading the Security Statement; no one would assume from the Security Statement that there was no room for improvement in SolarWinds' implementation of role-based access controls. They would instead expect that SolarWinds generally had procedures in place to limit users' access based on what they needed for their role—which it did—and that this policy objective also guided the company's efforts at continuous improvement—which it also did, as this episode illustrates.

131. *Security Researcher Report About Accidental Exposure of FTP Password.* Mr. Graff also points to an incident in 2019 in which a security researcher reported finding a SolarWinds password contained in a code repository that had accidentally been made publicly searchable on Github.¹⁷⁵ (Github is a cloud-based service used for storing code repositories.) The password was for an FTP account¹⁷⁶ on a server at Akamai (a third-party hosting service), which SolarWinds used to host a site where its software could be downloaded by customers.¹⁷⁷ Investigation revealed that the accidental publication of the code on Github was the result of human error by a SolarWinds intern, who was working on improving the functionality of the site.¹⁷⁸

132. As reflected in the email chain Mr. Graff cites, the incident was remediated immediately after it was reported, and investigation confirmed that the password had not been

¹⁷⁵ Graff Report ¶¶ 86-93.

¹⁷⁶ "FTP" stands for "File Transfer Protocol," which is a method used to transfer large files on the internet.

¹⁷⁷ See SW-SEC00407702 at -704.

¹⁷⁸ SW-SEC00407702 at -704 ("Engineering intern ... accidentally uploaded it to Github including configuration file that contained login and password for publishing files to Akamai.").

discovered or misused.¹⁷⁹ Further, any potential for misuse—in particular, any potential that the password could be used to upload malicious software to the site in question—was limited, because SolarWinds software is digitally signed by SolarWinds. Because companies installing new software typically check whether it has been digitally signed before installing it, any malicious software uploaded with this password would likely have quickly been detected as inauthentic.¹⁸⁰

133. Mr. Graff appears to infer from this incident that SolarWinds lacked role-based access controls. He states: “Clearly, if *the public* had access to this system, then role-based access controls were not in place (as the public had no ‘specific job function’ at SolarWinds that would necessitate access) and access to the system was not determined on a least privilege necessary basis (as the public should not have had this privilege).”¹⁸¹ This conclusion is, frankly, absurd. Obviously, SolarWinds did not intentionally grant “the public” access to the FTP account in question. Due to an *accident*, there was a *risk* that an unauthorized person could gain access to the account. But that does not imply that SolarWinds had a policy of freely allowing anyone to access the account or that it generally lacked processes and procedures for limiting user access based on their role. This incident really has nothing to do with whether SolarWinds had role-based access controls. By analogy, merely because an employee accidentally loses a key in the physical world does not imply that the company does not have locks on its doors or that it lacks procedures for distributing keys only to the employees that need them.

134. Mr. Graff also notes that, as part of the remediation of this incident, someone

¹⁷⁹ *Id.* at -704-05 (noting “[t]he compromised account was disabled on Akamai” the same day report was received, and confirming that “no one accessed Akamai using this account other than members of internal release management team”).

¹⁸⁰ *Id.* at 705-706 (explaining that “just to be 100% sure,” the release management team was checking to ensure there were “no modified files” on the download site, but “[b]ecause all of the [files distributed on the site] are signed by our certificate, the probability is very low”). By comparison, part of what made the SUNBURST attack so sophisticated is that the threat actor was able to compromise SolarWinds’ signing process itself and thereby pass off maliciously altered versions of the Orion software as if they were authentic.

¹⁸¹ Graff Report ¶ 86.

suggested that it “might make sense moving forward” to use a “special account only for MIB uploads with account rights limited only to this specific action.”¹⁸² There is no discussion in the document indicating what this meant or whether the suggested change was even feasible,¹⁸³ but in any event this appears to be an instance where SolarWinds was considering whether it was possible to fine-tune limits on one particular account—out of many thousands used within the company—related to a specific server. The fact that SolarWinds was considering ways to tighten access only shows, again, that it took the principle of least privilege seriously and was looking for a way to extend it further in this specific context, as part of thinking creatively about mitigations in the wake of an incident.

2. Mr. Graff’s Unwarranted Inferences from Isolated Notations in Documents

135. Aside from over-generalizing from isolated incidents, Mr. Graff also makes unwarranted inferences from isolated notations in documents, which he interprets without regard to context, witness testimony, or volumes of evidence contradicting his interpretation.

136. *Notation in Progress Slide on User Access Audit.* For example, Mr. Graff points to a slide deck from March 2018—again in draft form—containing slides with updates on various ongoing projects.¹⁸⁴ Mr. Graff points to a notation in one of the slides that reads “Concept of least privilege not followed as a best practice” and concludes this was “[i]n direct contradiction” with the Security Statement’s representation that access controls were “set on a need-to-know / least privilege necessary basis.”¹⁸⁵

137. Nowhere, however, does this document indicate that this notation was meant as any

¹⁸² *Id.* ¶ 90 (quoting SW-SEC00001476 at -483).

¹⁸³ *See* SW-SEC00001476.

¹⁸⁴ Graff Report ¶ 61 (citing SW-SEC00012266).

¹⁸⁵ *Id.* (quoting SW-SEC00012266 at -268).

sort of finding that SolarWinds generally did not set access controls on a least-privilege necessary basis.¹⁸⁶ The notation appears under the heading “Issues, Risks, & Dependencies.”¹⁸⁷ It is not clear that it was meant to be a finding at all, as opposed to being a statement of the concern that the project the slide described—an audit of user privileges—was meant to address. In other words, the notation could simply have meant that the purpose of the project was to *check* whether the concept of least privilege was not being followed as a best practice. Notably, the project start date was October 1, 2017 and a speaking note on the slide labeled “10/16/2017 Update” states “*Appropriate checks are in place to grant access* but audit of access is not consistently implemented.”¹⁸⁸ This indicates that processes *were* generally in place at the time to set access controls on a least-privilege-necessary basis, but there was a concern that access rights were not being sufficiently audited after the fact, which the project appears to have been intended to correct. The same page in the slide deck shows that, as of February 2018, SolarWinds was in the process of “[v]alidating privilege levels and access permissions,” and that it subsequently planned to “establish [a] repeatable security assessment methodology for continuous monitoring.”¹⁸⁹ This also indicates the purpose of the project was to conduct an audit of user access and create a consistent process for doing so going forward. Note that this was months before the Relevant Period began, and as I discussed earlier, there is evidence that user access reviews were regularly conducted by, and after, that time.

138. Not only does Mr. Graff ignore the context from the document, but he also ignores testimony about the notation from the person who wrote it—Eric Quitugua. To the extent I were conducting a security assessment and this notation raised any concerns for me, I would ask the

¹⁸⁶ See SW-SEC00012266.

¹⁸⁷ *Id.* at -268.

¹⁸⁸ *Id.* (emphasis added).

¹⁸⁹ *Id.*

responsible employees to explain what it means, rather than leaping to a conclusion that it shows some sort of enterprise-wide failure to implement the principle of least privilege. And Mr. Quitugua specifically testified that the notation “doesn’t indicate that it was a problem across the organization,” but rather only that it “may have been found that a particular system wasn’t following the concept of least privilege.”¹⁹⁰ Mr. Graff does not acknowledge or explain why he did not review or credit Mr. Quitugua’s testimony that this notation was not intended to convey any systemic problem.

139. Finally, Mr. Graff ignores all the evidence of the specific practices that SolarWinds *actually followed* in provisioning users with access rights during the Relevant Period. There is no need to try to figure out what those practices were by interpreting obscure notations in high-level slide decks. There is detailed testimony and large volumes of artifacts that make clear what those practices were. That is why, in conducting a security assessment, I would not typically rely on vague remarks in slide decks or emails to understand a company’s practices. I would instead engage the relevant individuals and look at the artifacts of those practices so that I could obtain a detailed understanding of them. Had Mr. Graff taken a similar approach here, it would be clear that SolarWinds took the principle of least privilege into account in provisioning users with access rights. The SARF process was designed for that very purpose.

140. *FedRAMP Preliminary Assessment.* Another document Mr. Graff cites is a document he describes as “an internal assessment of security controls” prepared by Kellie Pierce, whom Mr. Graff identifies as “Director of Security” at SolarWinds.¹⁹¹ Mr. Graff asserts that this document shows “SolarWinds lacked a policy to enforce least privilege and did not audit

¹⁹⁰ E. Quitugua Dep. Tr. at 219:20-25.

¹⁹¹ See Graff Report ¶¶ 40, 64 (citing SW-SEC00045358).

compliance with the least privilege principle.”¹⁹² Mr. Graff grossly mischaracterizes Ms. Pierce’s role at the company as well as this document, which, as witness testimony makes clear, is simply not a reliable source of information about SolarWinds’ security program.

141. Ms. Pierce was not the “Director of Security” at SolarWinds. She was a “program manager” who worked under Rani Johnson and Tim Brown.¹⁹³ As Ms. Pierce herself described it, her “entire role at SolarWinds” was a “coordination role.”¹⁹⁴ That is, she would help coordinate projects by gathering documentation and information from other people and tracking tasks to completion.¹⁹⁵ Ms. Pierce repeatedly emphasized at her deposition that she herself was “not a technical person” and had no substantive responsibility for SolarWinds security policies or practices.¹⁹⁶ As Jason Bliss, SolarWinds’ Chief Administrative Officer, testified: “Kellie was within the CIO office and she was a program manager. So Kellie’s role was more to make sure that the trains were running on time, that notes were taken accordingly, that materials were produced. She wasn’t a technical resource.”¹⁹⁷

142. Testimony also makes clear that the “internal assessment” prepared by Ms. Pierce that Mr. Graff cites was *not* undertaken in order to assess the state of SolarWinds’ security. Rather, as Ms. Johnson, Mr. Bliss, and Ms. Pierce all testified, the assessment was done in response to a request from SolarWinds’ cloud business line—a small portion of SolarWinds’ overall business—

¹⁹² *Id.* ¶ 66.

¹⁹³ T. Brown Dep. Tr. at 170:7-9.

¹⁹⁴ K. Pierce Dep. Tr. at 87:10-11.

¹⁹⁵ *Id.* at 18:22-25 (“I helped ... do a lot of the coordination work that was required across the company for the privacy—or the data privacy GDPR program.”); *id.* at 24:6-8 (stating “my role was really just to coordinate ... with the technical people”); *id.* at 33:6-7 (“Most of my role was around coordination and coordinating with the right people.”).

¹⁹⁶ *Id.* at 21:17-18; *id.* at 28:18-19 (“As I stated before, I’m not a technical person.”); K. Pierce Inv. Tr. at 176:23-24 (“I would coordinate the reports, but I’m not a technical person”); *id.* at 181:21 (“As I stated earlier I’m not highly technical”).

¹⁹⁷ J. Bliss Dep. Tr. at 32:20-25.

to determine how much cost and effort would be entailed in trying to obtain “FedRAMP” certification for SolarWinds cloud products.¹⁹⁸ As I know from my experience in the industry, FedRAMP is a highly demanding set of federal standards that cloud products must meet for the federal government to be able to purchase them. SolarWinds’ cloud business line wanted to be able to sell its products to the federal government, but Ms. Johnson believed that complying with FedRAMP would be “very expensive” because the standards were difficult to meet and would require extensive formal documentation approved by an outside third-party assessor.¹⁹⁹ It was in this context that Ms. Johnson asked Ms. Pierce to do a “very cursory, very preliminary” assessment of how much cost and effort would be involved in trying to obtain FedRAMP certification, as it was believed that the expected investment would not be worth the expected return from increased sales.²⁰⁰ In other words, the assessment was a *budgeting* exercise—not a security exercise.

143. While Ms. Pierce prepared the assessment by creating a spreadsheet of the 325 FedRAMP controls and inputting her comments as to whether she believed a “program” was currently in place for each, it is clear that the document is not—and was not meant to be—reliable at a granular level. As Ms. Pierce testified, she was “not a FedRAMP expert”²⁰¹ and did not “have

¹⁹⁸ R. Johnson Dep. Tr. at 194:13-16 (“This was a preliminary reaction to a request to make an investment in [F]edRAMP readiness for products that did not have a strong business justification.”); J. Bliss Dep. Tr. at 186:2-5 (explaining that the objective was to do a “quick, cursory, preliminary review as to how much do we think this is going to cost us? How much effort needs to go into this?”); K. Pierce Dep. Tr. at 48:3-5 (explaining that this was “a preliminary, very beginning, like, quick and dirty-type evaluation to see if the company wanted to invest in FedRAMP certification”).

¹⁹⁹ R. Johnson Dep. Tr. at 194:19-196:2 (“It was a very cursory collection of data ... because the formality and the requirement of leveraging a third-party assessment organization or a [third-party auditing organization] for [F]edRAMP is very expensive and you have to create years—at least a year of reporting documentation. ... What’s more, the—there was ... a hypothesis on Kellie’s part and certainly mine because she and I have run programs before to prepare companies for product certifications. The reality that these products don’t have the U.S.-based staffing infrastructure [required under FedRAMP] means that we knew that we would ... this would be too [expensive] of an effort. So this was a very cursory, very preliminary [stab] at [showing] this is gonna cost too much and not going to be worth the effort in this time frame.”).

²⁰⁰ *Id.*

²⁰¹ K. Pierce Dep. Tr. at 47:16; *see also* R. Johnson Dep. Tr. at 192:14-15 (“Kellie is not an auditor and has no expertise in this particular area.”).

a good understanding of what [the] language in the technical controls actually meant.”²⁰² Her comments were not meant to be “findings” but instead were “basically [her] best guess”²⁰³ from reading the language in each control and seeing if she recalled seeing similar language in SolarWinds policies she had reviewed in the past, through coordinating SOC-2 audits.²⁰⁴ It was, as she put it, a “quick and dirty” assessment.²⁰⁵ As Mr. Bliss testified, Ms. Pierce was “more or less spitballing” in order to come up with a rough estimate of “the scope of activities we would need to do to obtain FedRAMP compliance with our cloud properties and how long would that roughly take.”²⁰⁶

144. Mr. Graff does not mention any of this important context in his report, but instead treats the preliminary assessment prepared by Ms. Pierce as if it were an authoritative audit of SolarWinds cybersecurity posture. It clearly was not, and it does not support the inferences Mr. Graff seeks to draw from it.

145. First, Mr. Graff notes that, of the 43 FedRAMP requirements in the “Access Controls” family, Ms. Pierce indicated that she believed that a program only “may be in place” for 18, and that there was “no program in place” for 23, including four under the category of “least privilege.”²⁰⁷ Mr. Graff appears to treat these “ratings” as evidence that SolarWinds “lacked a policy to enforce least privilege”²⁰⁸ as represented in the Security Statement, but this inference

²⁰² K. Pierce Dep. Tr. at 125:19-23.

²⁰³ *Id.* at 60:17-19.

²⁰⁴ *Id.* at 28:13-25 (“I could find the NIST framework, put it in a document and often work with others to—for input and then make my—my best guess, not as a technical person and not as an auditor”); *id.* at 47:16-48:5 (“Q. And what was your involvement in the—assessing FedRAMP moderate controls, if any? A. Again, a coordination role”); *id.* at 125:11-18 (“Q. Did you rely on anything other than your memory of those policies based on your limited experience coordinating SOC 2 and ISO audits? A. No, I did not.”).

²⁰⁵ *Id.* at 48:4.

²⁰⁶ J. Bliss Dep. Tr. at 186:8-14.

²⁰⁷ Graff Report ¶ 64 (citing SW-SEC00045358).

²⁰⁸ *Id.* ¶ 66.

simply does not follow. For one thing, Ms. Pierce’s “ratings” cannot be considered accurate to begin with, given her lack of FedRAMP expertise. But even putting that aside, the FedRAMP requirements relating to access controls and least privilege go far beyond the representations in the Security Statement—again, FedRAMP is a very demanding certification standard. Moreover, many of the requirements relate to access controls on the cloud product at issue rather than access controls on SolarWinds’ network. So, even if FedRAMP’s requirements were not met by SolarWinds, that would not imply that SolarWinds was not meeting the much different, and lower, bar set in the Security Statement. Notably, with one exception, Mr. Graff does not discuss the details of the 43 FedRAMP requirements at issue or how they relate to anything the Security Statement says.

146. The only one of the FedRAMP requirements Mr. Graff specifically tries to relate to the Security Statement is a requirement stating: “The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.”²⁰⁹ Ms. Pierce marked this as a control SolarWinds “may have” in place and placed a comment stating: “This is included in the Access/Security Guidelines document. An audit that this is in place has never been performed.”²¹⁰ From this, Mr. Graff concludes that SolarWinds “did not audit compliance with the least privilege principle” and thus did not have “a way to verify whether the least privilege principle was being adhered to.”²¹¹

147. This conclusion only shows why Mr. Graff is wrong to place any reliance on this document at all. SolarWinds *did* audit its compliance with the least privilege principle, through

²⁰⁹ *Id.* ¶¶ 64-66 (quoting SW-SEC00045358, at tab “MODERATE SUMMARY KP,” Rows 17-22, tab “MODERATE kp METRICS,” cells D7-F8).

²¹⁰ SW-SEC00045358, at tab “MODERATE SUMMARY KP,” cell 17G, tab “MODERATE kp METRICS,” cell 9E (FedRAMP spreadsheet, August 28, 2019).

²¹¹ Graff Report ¶ 66.

the user access reviews that it regularly conducted, which looked specifically at what level of privilege each user in the company had.²¹² Indeed, Mr. Graff himself references some of these audits in other places in his report.²¹³ Moreover, these user access reviews were themselves audited as part of SOX audits of financially significant systems (including Active Directory), which validated that “[u]ser access privileges are re-validated on a quarterly basis to confirm that users maintain appropriate access.”²¹⁴ And one of the SOC-2 assessments that was prepared for SolarWinds specifically validated that “[t]he entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, *giving consideration to the concepts of least privilege* and segregation of duties, to meet the entity’s objectives.”²¹⁵

148. The SEC never asked Ms. Pierce any questions about her notation that “an audit” of the least privilege principle “has never been performed,” so it is unclear why she made this notation in the document. She may not have fully understood the meaning of the “least privilege” terminology; or she may have not been familiar with the user access reviews conducted by the company; or she may have simply not thought the issue through, since, as she testified, she only spent “a few minutes” going through each of the 325 FedRAMP controls.²¹⁶ But in any event, this just begs the question of why Mr. Graff is relying on an isolated comment in a spreadsheet, prepared in a “quick and dirty” manner by someone who acknowledged she was “not a technical person” and “not a FedRAMP expert,” in order to determine what SolarWinds’ practices were—

²¹² See, e.g., SW-SEC00147725; SW-SEC00235950; SW-SEC00296398. Note that the “Role” columns in each confirms the level of access for various users.

²¹³ Graff Report ¶¶ 61, 97 & n.180.

²¹⁴ PWC-SEC-00028649 (2020 PWC audit work papers, Overview tab, row 11); PWC-SEC-00017450 (2019 PWC audit work papers, 2.5 Access Review tab, rows 16-21).

²¹⁵ HOLTZMAN_0003092 at -108 (emphasis added).

²¹⁶ K. Pierce Dep. Tr. at 125:2-6 (“Q. So that’s would you say like a few minutes per control? A. Correct.”).

rather than simply consulting *direct evidence* of those practices that is available elsewhere. Again, Mr. Graff’s methodology does not reflect accepted practice in the industry. If I were hired as an outside consultant to conduct a security assessment of SolarWinds, I would never rely on a document like the preliminary assessment Ms. Pierce prepared. I would engage people with direct knowledge of the relevant practices and seek to review artifacts generated from the practices they described.

149. It is also worth pointing out that the Security Statement does not even represent that SolarWinds “audited” its compliance with the principle of least privilege. So even if SolarWinds did not conduct such audits—and there is clear evidence that it did—that would not imply that SolarWinds did not follow the principle of least privilege. Again, the SARF process was designed around the principle of least privilege. SolarWinds did not need to audit that process in order to know that it followed it. In fact, it is common for many practices that are part of a company’s cybersecurity program not to be audited, at least not formally; but that does not mean the practices are not in fact followed. While formal audit documentation would be needed for FedRAMP certification—which is likely why Ms. Pierce made reference to audits in her preliminary assessment—it was not required by the Security Statement. Notably, Ms. Pierce herself testified that there was nothing in the preliminary assessment that gave her “any reason to believe the Security Statement was inaccurate in any way.”²¹⁷

150. *User Access Management Tool Evaluation.* The last example I will cover of Mr. Graff taking a document out of context with respect to access controls is a presentation from January 2018, titled “User Access Management: Tool Evaluation & Recommendation.”²¹⁸ Mr. Graff cites a statement in this presentation that “there is no organization-wide, standardized

²¹⁷ *Id.* at 128:13-18 (“Q. Is there anything in the preliminary FedRAMP assessments you prepared that gives you any reason to believe the security statement was inaccurate in any way? A. No.”).

²¹⁸ Graff Report ¶¶ 78(a), 94, 109 (citing SW-SEC00043620).

approach to access management,” and concludes from this remark that there was a “lack of processes to implement role-based access control (as explicitly asserted by the Security Statement).”²¹⁹ That is not what the document is fairly read to say or what the evidence shows.

151. The document says there is no single “*organization-wide standardized* approach to access management”—not that there was a lack of processes generally.²²⁰ And the statement was made in the context of a presentation about finding a standardized technical *tool* that the company could use for provisioning and deprovisioning access across the company.²²¹ As several witnesses explained, a problem that the company was trying to solve at this time was that when someone was onboarded or offboarded, there would be multiple systems that help-desk personnel would have to configure in order to provision or deprovision the person with access.²²² While many applications they would need were accessible through Active Directory, others were not and would have to be separately configured. For example, some parts of the business used Google Cloud products, which had to be separately configured.²²³ Setting up accounts on different systems was tracked through the SARF process and the tickets that would be handled by IT help-desk staff—

²¹⁹ *Id.* ¶ 78(a) (quoting SW-SEC00043620 at -621).

²²⁰ SW-SEC00043620 at -621 (emphasis added).

²²¹ *Id.* at -622 (Slide titled “Tool Analysis” noting that “a group of IT Team members reviewed available tools that are currently used for user access management and others that may be used for this purpose”).

²²² R. Johnson Dep. Tr. at 103:14-21 (“Azure active directory ... was a replacement for an older technology, active directory on prem that was highly federated. The point of the identity and access management project, which put Azure AD in the cloud, was a way to centralize identity across all of the three different business units.”); J. Kim Dep. Tr. at 81:1-24 (“[T]here was a project around Azure AD which was a way for us to be able to look at that as a possible solution for us to be able to centralize identity and then utilize Azure’s AD capability for us to be able to then see how we can ... standardize things like access control. ... Because if you are using multiple tools and you are utilizing a lot of manual processes, you’re leaving room for people to accidentally make mistakes”); *see also* B. Cline Dep. Tr. at 140:13-15 (“[W]e had multiple processes in place around the onboarding and offboarding of users and their accounts.”).

²²³ *See* J. Kim Dep. Tr. at 84:4-11 (explaining that SolarWinds was “utilizing Google Identity for some of the products and then utilizing Microsoft Active Directory” for others); T. Brown Dep. Tr. at 112:5-8 (“So we had a Google Identity source and an Azure Active Directory identity source. We consolidated under the Azure source for truth.”).

which was a standardized process, but it was manual, which introduced potential for error.²²⁴ So the company was looking for a standardized *technical* approach that would minimize the number of systems that had to be separately configured.

152. That is the context for the presentation in question. The presentation looked at several different tooling options and recommended leveraging Microsoft Azure Active Directory (“Azure AD”) to standardize access provisioning.²²⁵ As the presentation notes, Azure AD has single sign-on (“SSO”) functionality, which allows integration of third-party services—including cloud services like Google Cloud, for example—so that users only need to sign on to their Azure AD account in order to authenticate to those third-party services.²²⁶ This avoids the need to manually provision users with separate accounts on the integrated third-party services, as instead Azure AD users can be automatically mapped to user accounts on those services.

153. Multiple witnesses explained this in deposition testimony. For example, Ms. Johnson testified that SolarWinds was seeking to achieve a “centralized and standardized ... single authoritative source of identity for the entire company versus having separate identity stores,” so that there was a “a single pane of glass” user identity could be managed through.²²⁷ Mr. Johnson explained that Azure AD, which “was very new technology” at the time, met this need, as it “provided the ability to have a single source of authentication across the company.”²²⁸ Similarly, Mr. Brown testified:

So we had ... manual processes for on-boarding employees and giving them rights to certain, uh, certain systems or certain applications. And that process worked, uh, but we had not automated that process with a tool. We were going through and, uh,

²²⁴ B. Cline Dep. Tr. 140:16-23 (“There was [a standardized process in place]. That’s where the Web Help Desk, the SARF that we’ve referred to, so the systems access request form, and that digital process that flowed through our Web Help Desk managed our onboarding and offboarding of all rights and identity for a standard user.”).

²²⁵ SW-SEC00043620 at -624.

²²⁶ *Id.*

²²⁷ R. Johnson Dep. Tr. at 102:25-103:4, 185:18-186:3.

²²⁸ *Id.* at 103:4-8.

consolidating—we still had a Google directory service and a Azure directory service. We were consolidating to Azure.²²⁹

Likewise, Mr. Bliss testified that the company was seeking to “make improvements in tooling” by “trying to bring Azure on line” so that identity management could be “standardized across the entire company.”²³⁰

154. In light of the context from the slide deck itself and this witness testimony, Mr. Graff has no basis to conclude from the document that there was a general “lack of processes” to implement role-based access controls.²³¹ The fact that SolarWinds was looking to *improve* its existing processes, by making them more automated and centralized, does not imply that it lacked processes altogether. The Security Statement said nothing about whether SolarWinds used a centralized identity management tool like Azure AD to provision users with access across all applications. It simply spoke to there being a process in place to assign resources to users based on their role. That was the SARF process. Again, there are abundant artifacts evidencing that the SARF process was in place during the Relevant Period.²³² I do not understand why Mr. Graff would use a methodology that ignores this direct evidence and instead strains to infer what the company’s practices were based on cursory remarks pulled out of context from miscellaneous documents.

155. I have a similar take on Mr. Graff’s reliance on notations in other documents indicating a desire to mature the company’s access controls, such as a NIST scorecard assigning a rating of “1” to authentication and identity management.²³³ As multiple witnesses testified, this

²²⁹ T. Brown Dep. Tr. at 208:8-14.

²³⁰ J. Bliss Dep. Tr. at 232:3-23.

²³¹ Graff Report ¶ 78(a).

²³² It is worth noting that the presentation at issue was from January 2018—ten months before the beginning of the Relevant Period—which raises a further question as to why Mr. Graff would rely on this document.

²³³ See Graff Report ¶ 78(c).

score was meant to highlight the company's ongoing efforts to centralize and automate the administration of user access controls through Azure AD and related projects.²³⁴ I know from my own experience that rollouts of centralized access management solutions like Azure AD across a company as large as SolarWinds take extensive time to complete, as integrations with numerous third-party applications have to be arranged, each of which has to be carefully planned and tested before full implementation. It is therefore understandable that the IT team would want to highlight for management the need to support this project over time—which is what Mr. Brown and Ms. Johnson, who came up with the score, testified was the intention behind it.²³⁵ Again, Mr. Graff ignores this testimony and treats the document as evidence that the company simply lacked role-based access controls, which is not what it says and is inconsistent with the abundant direct evidence of the operation of those controls.

D. Mr. Graff Does Not Show Any Systemic Failure to Implement Password Controls

156. Mr. Graff next addresses the issue of passwords, concluding that “SolarWinds did not, in the manner that was represented in the Security Statement, enforce the use of unique account IDs or conform to password best practices.”²³⁶ I disagree with this conclusion as well.

157. As discussed earlier, I reviewed artifacts showing that the company provisioned unique IDs to users, maintained a written password policy, and automatically enforced password

²³⁴ See J. Bliss Dep. Tr. at 234:5-11 (explaining this was a “subjective determination” meant to highlight to management “ongoing activities” around the “standardization of the identity management across all of SolarWinds and its properties,” including the migration to “Azure”); R. Johnson Dep. Tr. at 181:18-183:23 (explaining that the score was in reference to “the privilege access opportunity and the making Azure AD the authoritative source of identity”); T. Brown Dep. Tr. at 208:3-209:2 (explaining that the score reflected “significant projects” relating to identity management that were ongoing and that funding was required for, including “consolidating to Azure”).

²³⁵ See R. Johnson Dep. Tr. at 227:11-22 (“Active directory environments are very complex. Every system that provides authenticated access leverages this environment to provide users access. When there are multiple active directories, it means that a new service has to be stood up and every piece of software that authenticates off of that has to be reintegrated. That reintegration time period and retesting time period is not a short window. It’s an extensive project.”); T. Brown Dep. Tr. at 208:22-24 (explaining that “these projects will take a long time, multiple years, multiple times of investment”).

²³⁶ Graff Report ¶ 111.

complexity requirements as a best practice where it was technically feasible to do so.²³⁷ Those artifacts alone, in my opinion, are sufficient to validate the Security Statement’s representations regarding unique IDs and strong password requirements.²³⁸

158. Mr. Graff again appears to have excluded such evidence from his review. Instead, as with access controls, he focuses on a small number of events and notations in documents that, at most, suggest that SolarWinds occasionally identified gaps in its policies that were remediated.²³⁹ It is commonplace and expected—even for companies with the most stringent security regimes—to identify these sorts of issues from time to time. As Mr. Graff himself states: “[N]o organization has perfect cybersecurity and ... any organization diligently assessing its cybersecurity will uncover, from time to time, some issues”²⁴⁰ Accordingly, none of these events or documents Mr. Graff cites change any of my opinions because—even if Mr. Graff’s interpretation of them were accurate (which it is not in important respects, as explained below)—that would not undermine the evidence establishing that SolarWinds generally implemented password controls in a manner consistent with the representations in the Security Statement.

159. Below I address the specific records on which Mr. Graff relies, and errors I believe he makes, in concluding that SolarWinds did not implement unique account IDs or password controls.

1. Unique Account IDs

160. Mr. Graff states that he identified “several examples” where SolarWinds employees used “shared accounts,” and he concludes, on that basis, that SolarWinds did not provision

²³⁷ See *supra* Section V.D.

²³⁸ See *id.*

²³⁹ See Graff Report ¶¶ 116-136.

²⁴⁰ *Id.* ¶¶ 25, 50, 101, 136, 190.

employees with unique account IDs.²⁴¹ Mr. Graff’s conclusion does not follow. The Security Statement does not purport to guarantee that sharing of accounts never occurred at SolarWinds. Instead it merely states that SolarWinds “require[s] that authorized users be provisioned with unique account IDs.”²⁴²

161. As I noted earlier, the user access reviews I examined show that users were in fact provisioned with unique account IDs.²⁴³ I do not understand Mr. Graff to be genuinely disputing that. The mere fact that sharing of certain accounts was occasionally detected at SolarWinds does not imply that SolarWinds lacked a general practice of provisioning users with unique account IDs. It is impossible for any company to completely prevent the sharing of accounts, as there is always the possibility of human non-compliance. None of the documents Mr. Graff cites suggests that SolarWinds had any general policy or practice of allowing accounts to be shared. To the contrary, they show that SolarWinds did not allow sharing of accounts and took steps to prevent it.

162. *Notation in Progress Slide on User Access Audit.* First, Mr. Graff cites the same slide from the March 2018 draft slide deck discussed above,²⁴⁴ concerning an audit of user privileges the company was conducting at the time.²⁴⁵ Mr. Graff cites a notation under “Issues, Risks, & Dependencies” consisting of the phrase “use of shared accounts throughout internal and external applications.”²⁴⁶ Mr. Graff again jumps to the conclusion that this was a finding, as opposed to an issue of concern the audit was intended to address—i.e., one of its objectives was

²⁴¹ *Id.* ¶ 117.

²⁴² SW-SEC00466129 at -132.

²⁴³ *See supra* Section V.D.1.

²⁴⁴ *See supra* ¶¶ 136-139.

²⁴⁵ Graff Report ¶ 119 (citing SW-SEC00012266 at -268).

²⁴⁶ *Id.*

to check throughout internal and external applications for any use of shared accounts.²⁴⁷ Mr. Quitugua, who prepared the slide, in fact testified that this was what the notation was about. As he explained, the notation concerned “service account[s]”—which are accounts intended for use by an application, rather than individual users.²⁴⁸ (For example, if an application needs to access information from a database, it may need an account on the database to be able to do so. That account is called a “service account.”) Mr. Quitugua had discovered instances where service accounts intended for use by an application were being used by individual members of the relevant application team in the course of their work, which was not best practice.²⁴⁹ So he undertook an effort to identify any service accounts used in this way and “decommission” them wherever found, by rotating the passwords so that they could not be used by individuals.²⁵⁰ The slide at issue refers to this project, as it notes under “Action Required”: “Work with teams to decommission use of shared accounts.”²⁵¹ Mr. Quitugua testified that this work was completed within the timeline indicated on the slide, which identified Q1 2018 as the completion date for the work.²⁵²

163. In short, the slide does not indicate that SolarWinds sanctioned the use of shared accounts. Rather, it shows the opposite, as the audit the slide concerns was conducted in part to identify any service accounts that individual users were using and decommission them. That is

²⁴⁷ *Id.*

²⁴⁸ E. Quitugua Inv. Tr. at 289:20-290:21 (explaining that “service accounts” were “used to run automated scripting processes within the business applications”); *see also* E. Quitugua Dep. Tr. at 221:8-23 (explaining that a “shared account ... can be used by a computer to perform its function”).

²⁴⁹ *Id.* at 290:4-21 (“What we found was that these service accounts, which were purpose built to run processes, were also being used by, you know, users, and they also knew the credentials, right. So that case, we considered those accounts shared accounts, accounts that users should not have access to ...”).

²⁵⁰ *Id.* at 291:25-293:2 (explaining that the intent of the project was “to work with teams to decommission the use of those shared accounts,” by first identifying shared accounts and determining if they were needed by the application, and then “rotat[ing] the credentials” for the accounts so “they couldn’t be used as shared”).

²⁵¹ SW-SEC00012266 at -268.

²⁵² *See* E. Quitugua Inv. Tr. at 299:10-20 (“Q. And do you know when that issue was remediated? A. Again, it would have—it would have been in alignment with the milestones described here in the project.”); SW-SEC00012266 at -268 (showing Q1 2018 as “Finish” date for last milestone).

exactly what you would expect a well-functioning cybersecurity program to do in order to *enforce* a policy against sharing of accounts: identify a gap, investigate it further, and remediate it. Moreover, the email attaching the slide deck that Mr. Graff cites is from March 2018, some seven months before the Relevant Period. Mr. Graff does not point to any evidence that this limited gap had not been remediated by the Relevant Period, as Mr. Quitugua testified that it was.

164. *Notation in Email About Internal Audit.* Second, Mr. Graff cites an April 2018 email circulating the results of an internal audit that identified three systems for which there were “[s]hared SQL legacy account login credentials used.”²⁵³ Mr. Graff seems to believe that these accounts were user accounts, as he states in response to this email: “[I]f account credentials are shared, then they are not unique to *each user*.”²⁵⁴ But the email indicates that the credentials were instead for service accounts—again, accounts used by applications, not people. The concern was not that these accounts were shared among *users*, but rather that they were “shared among multiple dbs [i.e., database applications]/websites.”²⁵⁵ That could be problematic from a security-monitoring perspective because it would make it difficult, in reviewing logged activity from the accounts, to know which application or website was using the account at any given time. This concern therefore appears to have no connection whatsoever to requiring that “users” be provisioned with unique account IDs.

165. In any event, this email again does not reflect any policy of allowing accounts to be shared, whether by users or applications. Rather it shows SolarWinds detecting and remediating any instances of this issue happening. And it also shows the issue was very limited in scope. As Ms. Johnson testified at her deposition, the audit at issue covered *hundreds* of services within

²⁵³ Graff Report ¶ 120 (quoting SW-SEC00043080 at -082).

²⁵⁴ *Id.* (emphasis altered).

²⁵⁵ SW-SEC00043080 at -080.

SolarWinds.²⁵⁶ The fact that only *three* were found to involve any use of shared accounts only goes to show that this was, as she put it, “not a thematic problem.”²⁵⁷ And, again, this email is from April 2018 and lists “Q2 2018” as the targeted remediation date for the shared accounts.²⁵⁸ Thus, the email certainly does not indicate any “thematic problem” during the Relevant Period, which did not begin until October 2018.

166. *Email Chain About Developer Access to Billing Data for Test Purposes.* Finally, Mr. Graff cites the email discussed above²⁵⁹ concerning the developers working on improving SolarWinds’ billing system who requested “SuperUser” access to the system for the work.²⁶⁰ Mr. Graff focuses on the fact that the developers had previously been using credentials borrowed from a different SolarWinds employee who had “SuperUser” access.²⁶¹ But as the email itself indicates, this was flagged as a security violation, which is why the developers were requesting that “SuperUser” access be added to their own accounts.²⁶² The fact that it was flagged as a security violation shows that SolarWinds had a policy against users sharing accounts—not that it allowed it.

167. This is a recurring flaw in Mr. Graff’s analysis: He treats instances in which the company detected and remediated violations of a policy as evidence that the company *lacked* a policy. Instead, it is evidence of the opposite: Part of *having* a policy is using it as a standard to

²⁵⁶ R. Johnson Dep. Tr. at 239:15-19 (explaining that “[t]welve servers at the end of a multi-hundred service, and services can have many, many servers, but twelve servers are showing they have actions to follow up on at the end of a year-long GDPR readiness review”); *id.* at 241:4-8 (“And it’s not thematic across SolarWinds; it is, after reviewing hundreds of critical assets, twelve servers are—have remediation that was still necessary.”).

²⁵⁷ *Id.* at 241:4-15 (“[T]hat there’s only twelve remaining actions that are requiring remediation to report on is actually quite remarkable.”).

²⁵⁸ SW-SEC00043080 at -084.

²⁵⁹ *Supra* ¶¶ 121-123 (citing SW-SEC00254254).

²⁶⁰ Graff Report ¶¶ 79-85.

²⁶¹ *See id.*

²⁶² SW-SEC00254254 at -255-258 (“The main issue here is there was a request to DevOps to add IASP SuperUser access to BizApps team.”).

detect and remediate nonconformance. That is what SolarWinds did here. Mr. Graff points to no evidence that SolarWinds knew of frequent violations of its policy against sharing of accounts and simply ignored them.

2. Hard-Coding of Passwords in Configuration Files

168. Mr. Graff next asserts that SolarWinds hard-coded passwords into certain configuration files²⁶³ and argues that this contradicted the Security Statement, which he “interpret[s]” as “stating that SolarWinds comported with industry norms related to password best practices.”²⁶⁴ This argument is flawed in two ways.

169. As an initial matter, the Security Statement does not say anything about whether SolarWinds hard-codes passwords in configuration files, nor does it make any open-ended statement that SolarWinds follows all “industry norms related to password best practices.”²⁶⁵ As with the issue of “shared accounts,”²⁶⁶ Mr. Graff is reading into the Security Statement representations that it does not contain. All the password section of the Security Statement says relating to “best practices” is: “*Our password best practices enforce the use of complex passwords ...*.”²⁶⁷ Thus, the only “best practices” the Security Statement mentions relate to automatically enforcing password complexity. As I mentioned earlier, the most straightforward interpretation of this statement is simply that SolarWinds automatically enforced password complexity as a “best practice,” in the sense that this was the company’s preferred practice but it was not feasible on every system.²⁶⁸ The Security Statement does not represent that SolarWinds followed any other

²⁶³ A configuration file is a file that stores settings for a server or software application. “Hard-coding” a password into a configuration file refers to embedding a password needed by the server or software application in the file itself, in plain text. This poses security risks and is disfavored.

²⁶⁴ Graff Report ¶¶ 124-129.

²⁶⁵ See Graff Report ¶ 125; SW-SEC00466129.

²⁶⁶ See *supra* Section VI.D.1.

²⁶⁷ SW-SEC00466129 at -132 (emphasis added).

²⁶⁸ See *supra* Section V.D.3.

password-related “best practices.” And it seems especially implausible to read the Security Statement as representing anything about hard-coding of passwords in configuration files, because the section addressing passwords is focused on *user* passwords, whereas any passwords that would be hard-coded into configuration files would be passwords for service accounts, not user accounts.

170. In any event, Mr. Graff fails to point to any evidence showing that SolarWinds had any regular practice of hard-coding passwords in configuration files. Mr. Graff cites only two instances where this was identified, and in both instances the hard-coding was not allowed but instead was flagged for remediation.

171. *Notation in Email About Internal Audit.* First, Mr. Graff cites the same April 2018 email discussed above,²⁶⁹ discussing the results of an internal audit that, as Ms. Johnson explained, covered hundreds of SolarWinds systems.²⁷⁰ The audit found a mere *five* systems where credentials were stored in plain text in configuration files.²⁷¹ Thus, as with the “shared SQL legacy accounts,” this was not a pervasive problem but instead was limited to a small handful of systems that were flagged for remediation—again, well before the Relevant Period.²⁷² Identifying and remediating discrepancies is what an audit is conducted for, and it shows that SolarWinds *had* a policy against hard-coding credentials in configuration files, not that it lacked one.

172. *Security Researcher Report About Accidental Exposure of FTP Password.* Second, Mr. Graff cites the external report from a security researcher mentioned above,²⁷³ about an FTP password embedded in code that an intern had inadvertently made public on Github.²⁷⁴ This is the *only* instance of a hard-coded password that Mr. Graff identifies within the Relevant Period—out

²⁶⁹ See *supra* ¶¶ 164-165,

²⁷⁰ Graff Report ¶ 128 (citing SW-SEC00043080).

²⁷¹ See SW-SEC00043080 at -080-082.

²⁷² See *supra* ¶¶ 164-165.

²⁷³ See *supra* ¶¶ 131-134.

²⁷⁴ Graff Report ¶ 128 (citing SW-SEC00001476 at -484).

of thousands of passwords and millions of lines of code that SolarWinds would have. Mr. Graff provides no reason to believe this was anything other than an isolated instance of human error by a very junior employee.

173. Mr. Graff argues that, rather than being “a one-time accident,” this incident “illustrates more pervasive problems at SolarWinds as a whole,” because of its supposed “magnitude.”²⁷⁵ But both the premise and the logic of this argument are wrong. As for the premise, Mr. Graff overstates the magnitude of the incident. He states that the exposure of the password made it possible for hackers to distribute malware to SolarWinds customers,²⁷⁶ but he ignores compensating controls that were in place. As noted earlier, software issued by SolarWinds would bear the company’s digital signature, a form of validation that companies commonly check for before installing software updates; so any malware uploaded to the site by someone else would likely have been quickly detected.²⁷⁷ But regardless, whatever the “magnitude” of the error that was made here, it does not indicate anything about its *frequency*. Mr. Graff has no basis to simply assume that hard-coding of passwords was a “pervasive problem” at SolarWinds based on a single instance of it. Indeed, the fact that the 2018 audit mentioned in the prior paragraphs found only a very small number of hard-coded passwords after reviewing many hundreds of systems indicates that this was *not* a pervasive practice at SolarWinds.²⁷⁸

3. Password Complexity

174. Finally, Mr. Graff argues that SolarWinds failed to enforce the use of complex passwords in contradiction to the Security Statement.²⁷⁹ But the *only* instance he cites of a non-

²⁷⁵ *Id.* ¶ 91.

²⁷⁶ *Id.*

²⁷⁷ *See supra* ¶ 132 & n.180

²⁷⁸ *See* SW-SEC00043080 at -080-082; *supra* ¶¶ 164-165.

²⁷⁹ Graff Report ¶¶ 93(a), 130-134.

complex password is, again, the FTP password included in the code developed by the intern: “solarwinds123.”²⁸⁰ This isolated incident does not support the weight Mr. Graff tries to place on it for two reasons.

175. First, the incident does not contradict the representation in the Security Statement that SolarWinds’ “best practices enforce the use of complex passwords.”²⁸¹ As explained earlier,²⁸² the most sensible way to read this statement is that SolarWinds automatically required the use of complex passwords where it was feasible to do so, i.e., where the system could be configured to enforce password complexity. The main way that SolarWinds did this was through password complexity requirements enforced through Active Directory, which was the gateway to most of the applications used by SolarWinds personnel.²⁸³ However, the FTP password at issue was not for a system that would have been accessible through Active Directory. It was for an account on a third-party service run by Akamai.²⁸⁴ Mr. Graff provides no evidence that this third-party service even offered a functionality that could be configured to automatically require complex passwords on user accounts, or, if it did, whether the available complexity parameters would have blocked a password like “solarwinds123.” This instead appears to have been a situation in which SolarWinds had to rely on manual compliance with the company’s password policy (which required a password to contain symbols in addition to letters and numbers). And manual compliance is always subject to the possibility of human error.

176. Second, in any event this was, again, a *single* instance of an account having a non-complex password—out of many thousands of accounts that SolarWinds would have maintained

²⁸⁰ *Id.*

²⁸¹ SW-SEC00466129 at -132.

²⁸² *See supra* ¶ V.D.3.

²⁸³ *See supra* ¶¶ 66-68.

²⁸⁴ *See* SW-SEC00407702 at -704-706 (“He accidentally uploaded it to Github including configuration file that contained login and password publishing files to Akamai.”).

during the Relevant Period. Mr. Graff provides no basis to infer from this incident that the use of non-complex passwords was any sort of pervasive problem at SolarWinds. Indeed, it *cannot have been* a pervasive problem, given that SolarWinds enforced password complexity on Active Directory, which gated many of the applications used by SolarWinds personnel.²⁸⁵ Rather, by every indication, this was a one-off incident, not a systemic failure.

177. It is also worth noting that this isolated instance was caught because SolarWinds had effective channels available for external researchers to report security issues. A security researcher who found the password was able to flag it for SolarWinds through an established process the company had for receiving external reports.²⁸⁶ Within hours of it being received, the report was actioned by SolarWinds' InfoSec team, which immediately changed the password.²⁸⁷ This is what well-functioning cybersecurity programs do. No matter how mature a company's cybersecurity program is, there is *always* the potential for human error, including error resulting in the exposure of login credentials. That is why it is considered best practice for companies to have channels for external reporting of security vulnerabilities, such as bug bounty programs—because it is a given that companies can never catch all such errors themselves. In fact, the accidental exposure of credentials is one of the most commonly reported issues by security researchers.²⁸⁸ People in the industry understand that lapses like this happen from time to time. No one would expect otherwise in reading the Security Statement. What they would expect is for

²⁸⁵ See *supra* ¶¶ 66-68.

²⁸⁶ SW-SEC00001489 (automatically generated email from reporter's submission).

²⁸⁷ SW-SEC00001463 (email confirming someone was “changing the password right now,” within 12 hours of report being submitted).

²⁸⁸ See, e.g., *The 10 Most Common Bugs of 2021 So Far, and How to Find Them!*, Bugcrowd (Feb. 6, 2021), <https://www.bugcrowd.com/blog/common-bugs-of-2021/> (reporting that the most common bug reported through Bugcrowd, a leading bug-bounty platform, is exposure of credentials or other sensitive data, including “[p]asswords and secret keys in public Github repositories”); M. Meli et al., *How Bad Can It Get? Characterizing Secret Leakage in Public GitHub Repositories*, Network and Distributed Systems Security (NDSS) Symposium (Feb. 24-27, 2019), https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_04B-3_Meli_paper.pdf (explaining that leakage of passwords contained in Github repositories is a “frequent” problem).

SolarWinds to fix a non-compliant password if it were brought to the company's attention, which SolarWinds did here. That is evidence of SolarWinds' having a password policy, not lacking one.

E. Mr. Graff Does Not Even Argue That SolarWinds Failed to Conduct Network Monitoring

178. Mr. Graff does not contest that SolarWinds' representations regarding network monitoring were accurate. Instead, he states that, "within the documents that [he] reviewed, [he] found insufficient evidence either to evaluate SolarWinds' network monitoring practices or to evaluate whether SolarWinds personnel were aware of any deficiencies in this area or discordances with the related assertions in the Security Statement."²⁸⁹ Mr. Graff does not elaborate on this conclusion at all—by explaining, for instance, how he went about looking for relevant evidence.

179. I do not know why Mr. Graff was unable to locate such evidence, particularly in light of the volume of data and deposition testimony available to the SEC (and thus to Mr. Graff). Indeed, I have reviewed substantial volumes of evidence regarding SolarWinds' network monitoring, which amply demonstrate that the company implemented controls that were consistent with representations in the Security Statement.²⁹⁰ Some of this evidence came in the form of deposition testimony from SolarWinds employee Brad Cline, who was the Director and Senior Director of IT at SolarWinds during the Relevant Period, and for that reason, has critical insight into the company's security practices. For reasons I do not understand, Mr. Graff did not cite Mr. Cline's deposition testimony a single time in his Report, notwithstanding that Mr. Cline provided substantial testimony about the company's network monitoring practices.²⁹¹ And to the extent that Mr. Graff wished to obtain artifacts of the practices Mr. Cline or others described, he could have asked the SEC to identify those in the record, or to request them from SolarWinds.

²⁸⁹ Graff Report ¶ 24.

²⁹⁰ *Supra* Section V.E.

²⁹¹ *Supra* ¶ 80.

180. Mr. Graff’s failure to consider this evidence is consistent with the problematic methodology he applies throughout his entire Report, as I discussed above. It appears that Mr. Graff simply did not wish to consider direct evidence of the practices at issue, and instead only sought out emails or slides from presentations that, taken out of context, he thought would portray SolarWinds’ security practices in a negative light—and was unable to find anything specifically related to network monitoring. This is, of course, an improper and unreliable approach to conducting a cybersecurity assessment.

181. I also note that Mr. Graff’s conclusion (or lack thereof) regarding network monitoring is entirely inconsistent with the SEC’s allegations in the Amended Complaint. The SEC alleged that SolarWinds had “many critical network monitoring failures” that were supposedly “documented” in materials the SEC had reviewed.²⁹² It is therefore remarkable that Mr. Graff stated that he found no evidence to support these claims, and it raises the question why the SEC would have ever made such highly incendiary allegations against SolarWinds—itsself a developer of network monitoring software—without a basis to do so.

F. Mr. Graff Does Not Show Any Systemic Failure to Follow Secure Software Development Practices

182. Lastly, Mr. Graff challenges the section of the Security Statement addressing the company’s software development lifecycle, offering the opinion “that the practices SolarWinds described in internal documents were inconsistent, from a cybersecurity perspective, with certain assertions made in the Security Statement related to software development.”²⁹³ Mr. Graff bases this opinion on SolarWinds documents that he believes show that SolarWinds failed to “enforce the separation of the production environment from the development environment, or enforce

²⁹² Am. Compl. ¶¶ 149, 158.

²⁹³ Graff Report ¶ 137.

standard security practices throughout the software development process.”²⁹⁴ I disagree with this opinion.

183. Mr. Graff’s analysis and the documents he cites do not support his conclusions. The Security Statement represented that SolarWinds followed a software development lifecycle with a “defined methodology for developing secure software” that incorporated security testing throughout the process.²⁹⁵ As explained earlier, based on the artifacts and testimony I reviewed, including in particular the FSRs and results of vulnerability scans and penetration tests during the Relevant Period, those representations were clearly true.²⁹⁶

184. Mr. Graff again ignores the most pertinent artifacts and testimony and instead tries to extrapolate broadly from a small number of documents about marginal issues. None of these events or documents on which Mr. Graff relies changes any of my opinions because they do not undermine the evidence showing that SolarWinds built security into its software development lifecycle as the Security Statement describes.

1. SolarWinds Maintained Separate Development and Production Environments

185. Mr. Graff starts by making an argument that does not even relate to SolarWinds’ software development lifecycle, i.e., to the steps that engineers follow in developing software. He instead challenges the Security Statement’s representation that “SolarWinds maintains separate development and production environments.”²⁹⁷ That is an issue relating to the company’s network security, not its software development lifecycle—which is why it appears under the heading “Network Security” in the Security Statement.²⁹⁸

²⁹⁴ *Id.*

²⁹⁵ SW-SEC00466129 at -132.

²⁹⁶ *See supra* Section V.F.

²⁹⁷ Graff Report ¶ 150.

²⁹⁸ SW-SEC00466129.

186. Specifically, the separation of development and production environments refers to the separation of the part of a company’s network where engineers develop software—the “development environment”—from the part of a company’s network used to run its day-to-day operations—its “production environment” (which can also be referred to as its “corporate” environment). As noted in the guidance cited by Mr. Graff, separating these two environments is important from a network-security perspective, because development environments “are often configured less securely than production environments,” in order to give software engineers the flexibility they need to test software under various conditions.²⁹⁹ That creates the risk that “attackers may use this difference to discover shared weaknesses or as an avenue for exploitation”³⁰⁰; in other words, if there is no separation between development and production systems, an attacker that compromises a less securely configured development system could use it as a vector for penetrating the company’s network more broadly. Therefore, it is considered best practice to logically separate a company’s development environment from its production environment, by segregating them into different network zones, with a firewall sitting between them that restricts traffic from one entering into the other.

187. This is what the Security Statement represented SolarWinds did. It stated:

SolarWinds maintains separate development and production environments. Our next generation firewalls (NGFWs) provide adequate network segmentation through the establishment of security zones that control the flow of network traffic. These traffic flows are defined by strict firewall security policies.³⁰¹

In other words, the Security Statement represented that it separated the company’s development and production environments by establishing a separate network zone for each and regulating the

²⁹⁹ Graff Report ¶ 143(a) n.270 (quoting OWASP, *Secure Coding Practices: Quick Reference Guide*, November 2010, at 11); *see also id.* (quoting NIST SP 800-53, at 98 for the statement that “the management of development or test configurations requires greater flexibility”).

³⁰⁰ *Id.*

³⁰¹ SW-SEC00466129 at -131.

flow of traffic between them through the use of a next-generation firewall. The firewall would help to prevent an attacker from jumping from the development environment into the production environment.

188. I note that this representation is not among the representations in the Security Statement that the SEC challenges in its Amended Complaint. Nonetheless, for purposes of responding to Mr. Graff’s argument, I have reviewed evidence relating to this representation and, based on the evidence I have reviewed, it was true. Multiple witnesses testified that the company had separate network zones for its development environment and its production (or “corporate”) environment, and that it used firewalls to separate the two.³⁰² Moreover, I have reviewed a sample of SolarWinds’ firewall logs that were preserved from the Relevant Period, which show “DEV” and “CORP” as two different zones from which traffic is hitting the firewall, and various policies or “rules” regulating the flow of traffic between the two zones.³⁰³ This is clear evidence that SolarWinds logically segregated the two environments through the use of a firewall, exactly as the Security Statement described.³⁰⁴

³⁰² See E. Quitugua Inv. Tr. at 134:9-136:22 (“[T]here’s two domains at SolarWinds, a DEV domain and a TUL domain. One is considered production, and one’s considered development. ... Q. Okay. And so for example, between the DEV and the TUL domains, was there a firewall used to segment those two network zones? A. Yes.”); T. Brown Dep. Tr. at 104:9-14 (“Q. What is your understanding of what it means to have separate development and production environments? A. There were multiple high-level network zones that were in place - so a development zone, a production zone, a lab zone, and then additional kind of microsegmented areas within the network.”); *id.* at 105:4-6 (explaining that the company used “Palo Alto Nextgen firewalls” to separate the zones); B. Cline Dep. Tr. at 81:7-83:18 (“Q. ... You’re saying there’s – there’s a separate product development environment and a separate standard corporate production environment? A. Correct. ... Q. ... So how do you know that SolarWinds maintains separate development and production environments? A. As mentioned, we managed a lot of the firewall rules that would have controlled those environments.”).

³⁰³ SW-SEC-SDNY_00055443—SW-SEC-SDNY_00055444.

³⁰⁴ I also note that the SARF forms distinguish between an “Active Directory TUL account”—“TUL” was another term used to refer to the production environment—and an “Active Directory SWDEV account,” and indicate that, while all users would receive an “Active Directory TUL account,” only certain types of employees would receive an “Active Directory SWDEV account.” See, e.g., PWC-SEC-00025433 at -434 (listing “Active Directory TUL account” among standard system accesses for all employees, but “Active Directory SWDEV account” for only certain roles). This indicates that separate instances of Active Directory were set up for the development and production environments, which is consistent with the environments being maintained as two separate network zones.

189. Mr. Graff does not genuinely argue otherwise. Instead, he focuses, again, on the email chain from November 2019 discussed above, about SolarWinds developers conducting testing on live billing data in the company’s production environment,³⁰⁵ and he concludes from this that SolarWinds failed to segregate its development and production environments.³⁰⁶ Mr. Graff is conflating two very different issues. The fact that, for this particular project, SolarWinds developers were testing billing data *inside* the production environment (i.e., inside CORP) does not imply that SolarWinds did not logically segregate that environment from its development environment (i.e., DEV). They were still two separate zones, with a firewall between them.³⁰⁷ Therefore, the more loosely configured infrastructure within the DEV environment was not a threat to the CORP environment, as it might be if there were no separation between the two. In other words, an attacker still could not exploit weaknesses in machines in the DEV environment as an avenue for attacking machines in the CORP environment.

190. Instead, all that was happening here was that developers were working *inside* the production environment. They weren’t disabling the firewall between the production environment and exposing it to threats from the infrastructure in the development environment; they were simply logged into the production environment—with its more securely configured infrastructure—and testing a billing application on live data in that environment. Now, as I discussed earlier, this did pose a potential risk: The developers might accidentally modify the billing data, which, because it was live data, might cause inaccuracies in billing or financial

³⁰⁵ See *supra* ¶¶ 121-126.

³⁰⁶ Graff Report ¶¶ 150-162.

³⁰⁷ See B. Cline Dep. Tr. at 83:13-84:1 (“[Q.] So how do you know that SolarWinds maintains separate development and production environments? A. As mentioned, we managed a lot of the firewall rules that would have controlled those environments.”).

reporting.³⁰⁸ But that risk has nothing to do with any network-security concern about failing to segregate the DEV and CORP environments.

191. This is yet another example of Mr. Graff focusing on a one-off incident, which he misinterprets to begin with, and trying to make very broad generalizations that are simply unwarranted—all while ignoring far more direct evidence of the practices at issue. In short, Mr. Graff points to no evidence showing that SolarWinds failed to segregate its development environment from its production environment through the use of a firewall, as stated in the Security Statement. It clearly did that. The incident he points to is instead a red herring involving a distinct—and minor—issue. If anything, it only underscores that there *was* a development environment separate from the production environment. The very reason the incident arose was that, while software would typically be tested in the (segregated) development environment, it was not feasible to do so for the billing system at issue—which is why the developers sought a special exemption allowing them to work directly in the production environment instead.³⁰⁹

2. The Security Statement Did Not Represent Anything About How SolarWinds Developed Internal Software Applications

192. Mr. Graff next opines that the Security Statement’s representation that SolarWinds followed secure software development practices was inaccurate because software applications that SolarWinds built for its own *internal* use were not by default subject to the same development practices as the software it built and sold to customers.³¹⁰ The Security Statement does not even speak to this issue, however.

193. The Security Statement’s representations about the company’s software development lifecycle are about the processes it followed in developing the *products* it sold to

³⁰⁸ See *supra* ¶¶ 123-125.

³⁰⁹ See SW-SEC00254254 at -265 (explaining that “[t]he developers are developing in Production as the staging/dev environments are not suitable”). That was a judgment call Mr. Brown was entitled to make.

³¹⁰ See Graff Report ¶ 163.

customers. As the “Software Development Lifecycle” section states in the very first sentence: “We follow a defined methodology for developing secure software that is designed to increase the resiliency and trustworthiness of *our products*.”³¹¹ That is what customers reading the Security Statement would be focused on: whether the products they were buying or considering buying had been developed securely.

194. The Security Statement does not make any representations about the process SolarWinds followed in developing *internal* software applications that it used for its own business purposes. As Mr. Cline and Mr. Brown both testified, SolarWinds builds a number of such applications, used for things like managing sales or HR data.³¹² Those internal applications are referred to within in the company as “BizApps.”³¹³ As Mr. Brown specifically testified, they are not “products” that are sold to or used by customers, but rather are applications “solely used within SolarWinds.”³¹⁴ Customers would not be purchasing those applications, nor would they be running them on their own networks, where they might be exploited as an entry point if they were subject to compromise. So customers would not have particular reason to be concerned with the development lifecycle that went into those internal applications.

³¹¹ SW-SEC00466129 at -132 (emphasis added).

³¹² B. Cline Dep. Tr. at 15:6-13 (“Q. And what were you hired to do as the head of BizApps? A. The role for business applications is very focused on what it sounds like, they’re our business applications. So it’s primarily if you think of Salesforce, NetSuite, our HR and marketing application. So it’s very much focused on the application side that the business runs off of.”); T. Brown Dep. Tr. at 271:1-17 (“BizApps were produced *internal products or internal solutions*. ... [T]he BizApps applications were extensions to Salesforce applications often or extensions to Netsuite applications.” (emphasis added)).

³¹³ T. Brown Dep. Tr. at 270:23-271:6 (explaining that BizApps are “internal products or internal solutions”); *see also* B. Cline Dep. Tr. at 15:6-13 (explaining that BizApps are SolarWinds “business applications” and “very much focused on the application side that the business runs off of”).

³¹⁴ T. Brown Dep. Tr. at 271:7-9 (“Q. So were the BizApps sold to customers or were they solely used within SolarWinds? A. Solely used within SolarWinds.”).

195. Accordingly, BizApps are not the sort of software addressed by the Security Statement's representations about the processes used to develop the company's "products." Mr. Brown explained the distinction between BizApps from products in his investigative testimony:

Products are under SDL [secure development lifecycle], products that we ship are under SDL. Products that customers get are under SDL. We have a number of internally built solutions, we'll call them solution[s], that do things like support our billing, that help us manage our customers, that help us generate lists of customers to send emails to. So these are called Biz[A]pps, business applications.³¹⁵

Mr. Brown similarly testified that BizApps were not covered by the Security Statement's representation about secure software development:

Q. Were [BizApps] developed ... pursuant to SolarWinds' secure development lifecycle?

A. Uh, they—they were not products. So as the statement says, it's for products.³¹⁶

196. Mr. Brown also explained that, for technical reasons, it would not make sense to construe the representations in the Security Statement about the company's software development lifecycle to apply to BizApps, because BizApps are sometimes built as extensions on top of third-party applications, such as Salesforce (a popular software for managing sales information). It is not possible to do things like run vulnerability scans or penetration tests on those sorts of extensions, because SolarWinds does not control the third-party code or infrastructure they are built upon. As he stated:

The BizApps applications were ... extensions to Salesforce applications often or extensions to NetSuite applications. So the process is—process for development is—is different. Scanners don't work for those because it's—it's different.

Q. Do you have a view as to whether it would have been appropriate for the BizApps to be developed pursuant to ... SolarWinds' secure development lifecycle?

...

³¹⁵ T. Brown Inv. Tr., Vol. II, at 394:23-395:4.

³¹⁶ T. Brown Dep. Tr. at 271:10-13.

A. So again back to our statement, it's for products. A different statement would need to be created for BizApps applications because the tooling and the statements here of, uh, vulnerability testing don't apply.

...

Q. Why do you say it's not technically possible?

A. Vulnerability management as called out in the software development lifecycle is not available for Salesforce because Salesforce is a hosted application run by a third party. You can't do a scan against them. It just would be not possible to run them through the same process that we run through products that we develop.³¹⁷

197. Mr. Graff ignores that, in discussing SolarWinds' software development lifecycle, the Security Statement refers specifically to "our products"—a term that he himself uses in his report to refer to software sold to SolarWinds' customers.³¹⁸ Instead, he focuses on other language in that section, referring to "the entire software development methodology," and "all development activities"—arguing that these phrases are broad enough to cover development of even internal applications.³¹⁹ But he ignores the context at the beginning of the paragraph that makes clear these words are in reference to the development methodology and activities that go into developing "our products."³²⁰ Mr. Graff also cites an entirely different section of the Security Statement, stating that "customer and end-user assets as well as corporate assets" were "managed under our security

³¹⁷ T. Brown Dep. Tr. at 271:14–273:4. Mr. Graff questions this testimony, citing an email sent from Mr. Brown from June 2020 that stated "we are working to get all products in Bizapps under SDL." Graff Report ¶ 169 (citing T. Brown Inv. Tr., Vol. II, at 395:15-23) (testifying about the email). Mr. Brown explained, however, that this initiative was done merely "as a good practice," in order to "protect[] SolarWinds"—not because these were products being sold to customers. *See* Brown Inv. Tr., Vol. II, at 395:24-396:4. Mr. Brown also made clear that it wasn't possible to do this with "all" BizApps; rather, it depended on the circumstances, such as whether the application was an extension of third-party software. *Id.* at 395:13-23 (explaining that each internal application required its own "evaluation" to determine whether to "bring it under SDL").

³¹⁸ *See, e.g.*, Graff Report ¶ 37 ("During the Relevant Period, *SolarWinds' products* served approximately 275,000 customers globally, including, small businesses, large enterprises, and government organizations." (emphasis added)); *id.* ¶ 38 ("*SolarWinds offered a range of IT management products* designed to help businesses" (emphasis added)); *id.* ¶ 183 (stating that "[internal] applications [are] technically *not products*" (emphasis added)).

³¹⁹ *Id.* ¶ 163 (quoting SW-SEC00466129 at -132).

³²⁰ *See id.* ¶¶ 163-183; SW-SEC00466129 at -132 ("We follow a defined methodology for developing secure software that is designed to increase the resiliency and trustworthiness of *our products*." (emphasis added)).

policies and procedures,”³²¹ but this language appears in the “Asset Management” section of the Security Statement, which relates to inventorying and maintaining a company’s IT assets (e.g., keeping track of all devices deployed on the network, wiping a system’s memory when decommissioning it, etc.).³²² It has nothing to do with software development, and does not provide any basis to infer that SolarWinds applies its software development lifecycle to all of its “assets,” which would not make sense given that most “assets” are not software applications.

198. In short, the Security Statement does not say anything about how the company develops its own internal software applications. For this reason, Mr. Graff’s criticism of SolarWinds for not developing the Orion Improvement Program, or “OIP,” through the software development lifecycle described in the Security Statement is another red herring. Mr. Graff spends many pages on this issue—it is the bulk of his argument that the Security Statement’s representations about SolarWinds’ software development lifecycle were false.³²³ But the entire argument is misplaced because OIP was an internal application—a BizApp—that those representations did not address in the first place.

199. As Mr. Brown explained extensively during his investigative testimony, OIP was one of SolarWinds’ BizApps, which SolarWinds used to collect Orion usage information from customers who agreed to provide it, in order to help advise customers on how to improve their deployment of the software.³²⁴ OIP was not software that SolarWinds *customers* used; it resided on SolarWinds own network and was used *by SolarWinds*. Mr. Graff seems to misunderstand this in stating that, “while it is true that OIP was not a stand-alone product that customers outright

³²¹ Graff Report ¶ 167 (quoting SW-SEC00466129 at -129).

³²² See SW-SEC00466129 at -129.

³²³ See Graff Report ¶¶ 163-183.

³²⁴ T. Brown Inv. Tr., Vol. II, at 395:3-7 (“So these are called Bizapps, business applications. One of those business applications is OIP. That business application was built internally for the specific purpose of collecting information and helping customers with their deployment.”).

purchased from SolarWinds, OIP was nevertheless used by customers,” and that “OIP was a component made available for customer installations of Orion.”³²⁵ These statements are incorrect: OIP was not a “component” of the Orion software that ran on customer systems, nor was it otherwise “used” by customers. OIP was an application that SolarWinds ran on its own server and that SolarWinds used for its own business purposes. As Mr. Brown explained in his investigative testimony:

[T]he OIP server that’s talked about is our internally-hosted server That’s what OIP is. . . . [I]t’s something inside of our environment. It’s not a product we sell, it’s not a solution that is, you know, offered to customers or anything like that. The OIP server sits inside of our environment and it takes information from clients to essentially improve their product. But it’s a separate application, not something that’s commercial. It’s something that’s inside of our environment to talk to.³²⁶

200. In other words, Orion customers had the option to agree to *send* their Orion usage data *to* OIP; but the application itself ran on SolarWinds’ internal network, where it was used by SolarWinds to analyze customer deployments. By analogy, if a customer sends a company product feedback via email, and that feedback gets logged in a customer-support application that the company runs on its network and uses to improve its services, that does not mean that the customer-support application is a “component” of the product sold to the customer or that the customer “uses” the application.

201. Because the OIP application was neither a component of a product sold to customers nor otherwise used by customers, it is not within the scope of the language in the Security Statement relating to SolarWinds’ software development lifecycle. That language told customers what went into the security of the “products” they were buying from SolarWinds and running on their network.

³²⁵ Graff Report ¶ 170.

³²⁶ T. Brown Inv. Tr., Vol. II, at 380:21-381:4; *see also id.* at 384:12-14 (“The OIP service, again [is] not something we ship to clients, not something we ship to customers.”); R. Johnson Inv. Tr., Vol. II, at 207:13-16 (“Q. And what is your understanding of what the Orion Improvement Program is? A. It was a server that collected information related to customers’ usage of Orion.”).

OIP was not a product they were running on their networks—it was an internal application running on SolarWinds’ network—so customers would not have the same concern with respect to it, and the language in the Security Statement simply did not address it.

202. Not only is Mr. Graff’s extended discussion about OIP irrelevant for this reason, but Mr. Graff also misportrays other facts in the course of his discussion. In support of his claim that vulnerabilities in OIP “pose[d] a significant threat,” Mr. Graff cites a handful of emails in June and July 2020 about potential vulnerabilities in OIP.³²⁷ Without context, Mr. Graff gives the impression that employees across the organization each independently voiced security concerns about OIP. That is not the case. In fact, all of the emails come from essentially one email chain, prompted by SolarWinds’ investigation of an incident reported by the Department of Justice’s U.S. Trustee Program (“USTP”).³²⁸ This is the same incident involving the USTP that is discussed in the SEC’s Amended Complaint.³²⁹ That incident involved suspicious activity on the USTP’s Orion server, in which malicious code seemed to be communicating from the Orion server through the channel that would typically be used to send usage data to OIP. As Mr. Brown explained at length in his investigative testimony, in initially responding to the report, his team was concerned that an attacker might be trying to *attack SolarWinds* through the OIP server. In that context, SolarWinds’ engineers brainstormed about any potential vulnerabilities that might exist in OIP, in order to ensure OIP was adequately hardened against attack. As Mr. Brown testified:

So our theory with this is that ... either the box [i.e., server] that [USTP] installed [Orion] on was a dirty box and had [malicious code on it], or that, you know, the box itself had been compromised without us and that that [malicious code] was attacking SolarWinds with that OIP layer. So that’s why you’ll see a lot of

³²⁷ Graff Report ¶¶ 172-177 (citing SW-SEC00024906; SW-SEC00000673).

³²⁸ See SW-SEC00024906 (Email thread with subject line: “SDL and Orion Improvement Program”); SW-SEC00000673 (Email thread with subject line: “SDL and Orion Improvement Program”).

³²⁹ See Am. Compl. ¶¶ 268-278.

hardening on OIP. ... We essentially brought in everybody to look at this traffic and this incident.³³⁰

As Mr. Brown explained, as part of this effort, the team applied the same sort of testing that it would do as part of its software development lifecycle for customer products to OIP—not because OIP was such a product or because the testing was supposed to have been done earlier, but because this particular incident raised a concern that OIP was potentially being targeted as part of an attack *on SolarWinds*:

[W]hen you build a product for internal use, not a product but a service that you're going to use internally[,] that doesn't necessarily follow the same processes that when we build the products from the outside. But we implemented a number of those processes around the OIP server and investigated the server itself and then, you know, made some changes to the OIP server to make sure that—you know, that it was hardened against attacks. Although we couldn't tell what the attack was from the data we had, [we] essentially looked everywhere we could and put as many safeguards in place on the OIP server so it wouldn't affect us.³³¹

203. This is exactly what I would expect a well-functioning cybersecurity program to do in this scenario, where there was a specific indication of a threat actor targeting the OIP server as a potential entry vector into SolarWinds: aggressively investigate every possible weakness in the OIP server to ensure that it was adequately protected. As it turns out, the entire exercise was a fire drill, as SolarWinds found no signs of compromise on the OIP server, and, as was eventually learned, the incident did not actually involve any attempt to compromise the OIP server.³³² Rather, the malicious code on the USTP's Orion server was SUNBURST, which was designed to obfuscate the traffic it sent to its command-and-control server by making it *appear* as if it were traffic being sent

³³⁰ T. Brown Inv., Vol. II, Tr. at 381:18-382:9.

³³¹ *Id.* at 388:10-21.

³³² See T. Brown Inv. Tr., Vol. II, at 405:15-20 (“So I think our investigation didn’t show any inappropriate activity to the OIP server. ... [Y]ou don’t see that this had an effect on our OIP sever internally.”).

to OIP.³³³ There was thus no vulnerability in OIP that had anything to do with the USTP incident, or SUNBURST more broadly.

204. In short, this is another non-event that Mr. Graff misportrays as a major issue. SolarWinds never represented in the Security Statement that it subjected its own internal applications to the same sort of security testing used to develop its customer-facing products. The fact that it voluntarily did so with respect to OIP in response to this particular incident was part of a laudable effort to aggressively respond to a specific potential threat. Mr. Graff has no basis to characterize the incident as evidence that anything in the Security Statement was false.³³⁴

3. SolarWinds Conducted Security Testing as Described in the Security Statement, and It Also Conducted Threat Modeling (Which the Security Statement Does Not Mention)

205. Finally, Mr. Graff opines that “SolarWinds’ internal communications” show that it (i) did not consistently implement threat modeling as part of software development and (ii) did not conduct penetration testing “a hundred percent of the time.”³³⁵ Once again, Mr. Graff, for reasons he does not explain, simply excludes from consideration the testimony and artifacts reflecting the security testing that SolarWinds conducted as part of its software development lifecycle,³³⁶ and instead relies on statements taken out of context.

³³³ T. Brown Inv. Tr. at 381:5-17 (“[T]he threat actor did work in order to, you know, mimic our protocol and try to make it look like OIP traffic.”).

³³⁴ It bears mentioning that the presence of vulnerabilities in a piece of software is common and expected, and does not necessarily imply poor design. For example, the CVE Program (short for “Common Vulnerabilities and Exposures”), sponsored by the Department of Homeland Security, has a website that catalogs software vulnerabilities, which currently number 240,830. See CVE, <https://cve.mitre.org/> (last visited Nov. 21, 2024). Major software companies frequently release patches for their products, with Microsoft, for example, releasing patches the second Tuesday of each month. See, e.g., *Patch Tuesday, October 2024 Edition*, [Krebs on Security](https://krebsonsecurity.com/2024/10/patch-tuesday-october-2024-edition/) (Oct. 8, 2024), <https://krebsonsecurity.com/2024/10/patch-tuesday-october-2024-edition/> (“Microsoft today released security updates to fix at least 117 security holes in Windows computers and other software, including two vulnerabilities that are already seeing active attacks. Also, Adobe plugged 52 security holes across a range of products, and Apple has addressed a bug in its new macOS 15 ‘Sequoia’ update that broke many cybersecurity tools.”).

³³⁵ See Graff Report ¶¶ 184-188 (quoting T. Brown Dep. Tr. at 134:10-22).

³³⁶ See *supra* ¶¶ 90-97.

206. First, Mr. Graff cites a remark in a May 2018 email from Mr. Colquitt, stating “we are just barely beginning to understand how teams are going to be doing [threat modeling].”³³⁷ As an initial matter, Mr. Colquitt’s statement could not undermine anything in the Security Statement because the Security Statement does not even mention “threat modeling.” Mr. Graff points to the more general representation in the Security Statement that SolarWinds “follows standard security practices including vulnerability testing, regression testing, penetration testing, and product security assessments,” and interprets that as a representation that SolarWinds also did threat modeling.³³⁸ But this interpretation is another example of Mr. Graff trying to read representations into the Security Statement that it does not make. Regardless of whether Mr. Graff believes that threat modeling is a “standard security practice,” the Security Statement did not make any open-ended statement that the company follows “all” “standard security practices”—which would be vague, since people in the industry have different conceptions of what is standard. The Security Statement instead specified which “standard security practices” the company followed with respect to software development—namely, vulnerability testing, regression testing, penetration testing, and product security assessments. As discussed above, the evidence clearly shows that SolarWinds followed those practices. The fact that Mr. Graff chooses to focus on “threat modeling” instead indicates, to me, that he cannot find evidence to show that SolarWinds did not follow those practices, so he is attempting to change the subject.

207. In any event, Mr. Graff ignores evidence in the record that SolarWinds did conduct threat modeling as part of its secure software development processes. “Threat modeling” is a loose term that can encompass virtually any effort to anticipate and address potential security threats as part of the software design process. For example, the OWASP Foundation, a well-recognized

³³⁷ Graff Report ¶ 185 (citing SW-SEC00237608 at -608).

³³⁸ Graff Report ¶¶ 184-185 (quoting SW-SEC00466120 at -132).

authority on software security, defines threat modeling as essentially a process for asking the following four questions:

- What are we working on?
- What can go wrong?
- What are we going to do about it?
- Did we do a good job?³³⁹

As OWASP states, “[t]here are many methods or techniques which can be used to answer each of these questions,” with “no ‘right’ way” that one must use.³⁴⁰

208. Mr. Colquitt similarly explained at his deposition that threat modeling is “inherent” in assessing and addressing security risks in software: “[W]hen I assess a particular requirement, I identify a risk and I mitigate that risk, that is threat modeling.”³⁴¹ As he stated, there is no one way to do this: “Threat modeling can be done verbally, it can be done on a piece of paper, it can be done on a whiteboard or you can use a formal tool to produce that documentation. There’s multiple ways to do this exercise.”³⁴²

209. Mr. Kim and Mr. Colquitt both testified that SolarWinds did threat modeling as part of the software development process, even if there was no one standardized way in which it would be done or documented.³⁴³ As Mr. Colquitt noted, the very fact that SolarWinds’ products “had security controls in them” is by itself evidence of threat modeling, because “[t]hose security controls are the outputs of a threat model having taken place.”³⁴⁴ Moreover, as Mr. Brown noted

³³⁹ OWASP Threat Modeling Project (last visited Nov. 22, 2024), <https://owasp.org/www-project-threat-model/> (section on “Threat Modeling - Four Question Framework”).

³⁴⁰ *Id.*

³⁴¹ Colquitt Dep. Tr. at 65:16-23; *see also id.* at 165:10-12 (“I would say that as an inherent aspect of implementing a mitigation to a security risk is inherently a threat modeling.”).

³⁴² *Id.* at 145:2-8.

³⁴³ *See* J. Kim Dep. Tr. at 148:12-24 (“[W]e were doing threat modeling between the products. That specific process was not standardized across the different parts of the organization. ... [B]ut I know that threat modeling was being done in the company.”); *id.* at 203:1-2 (“[A]bsolutely we were doing threat modeling.”); S. Colquitt Dep. Tr. at 66:10-13 (“[Q.] [I]n your experience, ... was threat modeling ... done internally by SolarWinds employees? A. Absolutely.”)

³⁴⁴ S. Colquitt Dep. Tr. at 206:15-207:2.

in his deposition testimony, SolarWinds had a dedicated architecture team in place, consisting of “very senior engineers,” whose job it was to conduct “design reviews” in order to ensure “that things were designed appropriately.”³⁴⁵

210. I have also seen evidence of threat modeling in the FSRs that I have reviewed. The FSRs have sections addressing security design considerations, with such headings as “Proactive Review of all FAS (High Level Design) Documents,”³⁴⁶ “Documents with security design implications,”³⁴⁷ or “Security related features identified by teams.”³⁴⁸ This shows that development teams were thinking about security during the design phase and building in features to address anticipated security risks, which would be a form of threat modeling. Indeed, some FSRs include documents specifically labeled “Threat Model.”³⁴⁹ Some of the FSRs also include design reviews by the Architecture Team, further reflecting consideration of security at the design stage. Moreover, the sample JIRA tickets linked to the FSRs that I have reviewed show risks being identified and fixes being proposed—again, a form of threat modeling.³⁵⁰ All of this evidence is consistent with the testimony of Mr. Kim and Mr. Colquitt that SolarWinds did threat modeling.³⁵¹ Indeed, as Mr. Colquitt explained, it is hard *not* to do threat modeling in some form if security is being considered during the software development process—as it clearly was at SolarWinds—because consideration of security inherently involves thinking about potential security risks and

³⁴⁵ T. Brown Dep. Tr. at 125:18-162:12.

³⁴⁶ See, e.g., SW-SEC-SDNY_00069825 at -825.

³⁴⁷ See, e.g., SW-SEC-SDNY_00055006 at -006.

³⁴⁸ See, e.g., SW-SEC-SDNY_00055028 at -028.

³⁴⁹ See, e.g., SW-SEC-SDNY_00055225.

³⁵⁰ See, e.g., SW-SEC-SDNY_00191599; SW-SEC-SDNY_00191618; SW-SEC-SDNY_00191853; SW-SEC-SDNY_00192020; SW-SEC-SDNY_00192221; SW-SEC-SDNY_00192346; SW-SEC-SDNY_00192747; SW-SEC-SDNY_00192845.

³⁵¹ S. Colquitt Dep. Tr. at 66:10-13 (“Q. But in your experience, ... was threat modeling ... done internally by SolarWinds employees? A. Absolutely.”); J. Kim Dep. Tr. 148:23-24 (“I know that threat modeling was being done in the company.”).

potential mitigations for them.³⁵²

211. With respect to Mr. Colquitt’s email, it appears to me that Mr. Graff takes this email out of context and, for reasons he does not explain, ignores the sworn testimony of witnesses—including Mr. Colquitt himself—who explained what this statement actually meant. As Mr. Colquitt explained in his deposition, when he wrote this email, “[t]hreat modeling ... was already happening.”³⁵³ In saying that “we are just barely beginning to understand how teams are going to be doing this activity,” he was not “talking about doing the threat modeling itself,” but was rather talking about how teams were going to be *documenting* that activity.³⁵⁴ At the time he was engaged in a project to improve documentation of SolarWinds’ software development practices and wanted to “determine what options we had in terms of producing [] documentation” of threat modeling and “tracking that documentation.”³⁵⁵ That is consistent with the context of the email, in which Ms. Johnson forwarded a list of *tools* that SolarWinds was using for various security functions (including penetration testing and vulnerability scanning) and asked Mr. Colquitt about threat modeling, which was not on the list.³⁵⁶ Thus, as Mr. Colquitt testified, he was explaining that threat modeling was a “process” (not something that would necessarily be accomplished with a tool, like vulnerability scanning) and that they were just beginning to think about how to “improve the process” with respect to documentation outputs.³⁵⁷ I therefore see no basis for Mr. Graff to consider this email as evidence that SolarWinds simply did not do threat modeling. Engineers often perform

³⁵² See *id.* at 141:21-25 (“You could potentially put threat modeling anywhere. It’s just an additional activity that you may choose to do informally or formally, but inherently it just happens as part of the software development process.”).

³⁵³ See *id.* at 142:16-19.

³⁵⁴ See *id.* at 142:1-19.

³⁵⁵ See *id.*

³⁵⁶ See SW-SEC00237608 at -608-609.

³⁵⁷ See S. Colquitt Dep. Tr. at 142:7-10 (“I wanted to improve the process. I was trying to determine what options we had in terms of producing that documentation and tracking that documentation that I had not yet settled on.”); *id.* at 144:23-145:8 (explaining that “I was implying that I wanted to improve the process,” which would not necessarily involve a “formal tool”).

many activities without formally documenting them. The fact that Mr. Colquitt was thinking about how to improve documentation of threat modeling does not imply that threat modeling was not already being done.

212. The only other document Mr. Graff cites relating to threat modeling is a “high level assessment” relating to three products within SolarWinds’ MSP business—RMM, Backup, and NCentral.³⁵⁸ Mr. Graff cites a notation in the assessment that “[n]o threat modelling [sic] nor analysis is performed as part of any process (except MSP Backup Engineering).”³⁵⁹ Mr. Graff states that this is a “severely problematic finding,”³⁶⁰ but without more context I do not believe he has a basis to draw that conclusion. It is unclear exactly what was meant by the remark in the document. As noted above, “threat modeling” is a broad term and can be done lots of different ways. The authors who wrote this assessment (who were not deposed) may have had in mind a *formalized* type of threat modeling that they wanted to be done, rather than meaning to say that no type of threat modeling was being done in any sense. It is also not clear what the basis was for the remark or to what extent the authors had surveyed the relevant engineering teams to fully understand what they might be doing related to threat monitoring, so it is difficult to gauge whether the remark was based on accurate information.

213. Notably, the evidence I have reviewed contradicts the remark that “[n]o threat modelling [sic] nor analysis is performed as part of any process”—at least if the remark is construed in the categorical way that Mr. Graff reads it. In particular, the FSRs that I have reviewed include FSRs for software releases of N-Central, RMM, and Backup—the three MSP products that are the

³⁵⁸ SW-SEC00166790 at -792.

³⁵⁹ Graff Report ¶ 186 (quoting SW-SEC00166790 at -794).

³⁶⁰ *Id.*

subject of the cited assessment.³⁶¹ These FSRs show that the development teams were doing threat modeling, in that they were identifying security risks to the software and developing mitigations for them. This is reflected, among other places, in the sections of the FSRs concerning “Vulnerabilities Addressed in Current Release,” which lists various “risks” that were identified during the development process and the “fix” or “mitigation” proposed or implemented for each.³⁶² The FSRs include entries of this sort from or before July 2019³⁶³—which is when the assessment cited by Mr. Graff was prepared.³⁶⁴ This leads me to believe that the remark Mr. Graff relies upon is either misinformed or was not meant to be read in the overly literal way Mr. Graff is reading it. Once again, this shows the basic flaw in Mr. Graff’s methodology, in that he chooses to rely on isolated remarks in high-level documents rather than examining the underlying artifacts of the relevant practices themselves.

214. Mr. Graff ends with perhaps his weakest opinion—that the Security Statement’s representation that SolarWinds conducted penetration testing was false because Mr. Brown testified that it “*may not* have been ‘done a hundred percent of the time.’”³⁶⁵ One hundred percent is not the appropriate standard, as Mr. Graff himself acknowledges.³⁶⁶ And as Mr. Brown made clear, “penetration testing *was definitely done*”; he was simply claiming he had not himself done “an exhaustive audit of” it.³⁶⁷ Mr. Graff cannot even provide an example of any instance when penetration testing did not happen. Instead, he just relies on one person’s acknowledgment that (of

³⁶¹ See, e.g., SW-SEC-SDNY_00055149 (“Final Security Review RMM Core 2020.4”); SW-SEC-SDNY_00069744 (“Final Security Review n-Central 2020.2”); SW-SEC-SDNY_00069751 (“Final Security Review Backup 2020.2”).

³⁶² See, e.g., SW-SEC-SDNY_00074874 at -877.

³⁶³ See *id.*

³⁶⁴ See Graff Report ¶ 186; SW-SEC00166790 at -790.

³⁶⁵ Graff Report ¶ 188 (citing T. Brown Dep. Tr. at 134:10-22) (emphasis added).

³⁶⁶ Graff Report ¶ 50 (“My decades of experience have taught me that no organization has perfect cybersecurity and that any organization diligently assessing its cybersecurity will uncover, from time to time, some issues needing to be addressed.”).

³⁶⁷ T. Brown Dep. Tr. at 134:10-22 (emphasis added).

course) there could *possibly* have been an example across all of SolarWinds’ software development over a multi-year period.

215. The only other evidence Mr. Graff cites with respect to penetration testing is testimony from a SolarWinds employee, Harry Griffiths, who stated that on occasion a customer would do their own penetration testing and find vulnerabilities that SolarWinds’ penetration testing did not.³⁶⁸ But the fact that SolarWinds and its customers may have identified separate vulnerabilities through their respective penetration testing is unsurprising, and if anything, just reinforces that SolarWinds was in fact doing its own penetration testing. As Mr. Griffiths stated in his testimony, and I agree, different penetration testing tools may identify different vulnerabilities, but that does not mean one tool or the other is insufficient.³⁶⁹ Moreover, it is not only common, but inevitable, that software will contain vulnerabilities after being released, even if the software has been subjected to rigorous testing during the development process. Complex software runs on codebases often consisting of hundreds of thousands, or even millions, of lines of code, which can interact with one another in unanticipated ways. As a result, a company cannot ever hope to identify all vulnerabilities that reside in the software. That is why companies like Microsoft, Google, and Adobe, report hundreds of vulnerabilities in their software, post-release, every year.³⁷⁰ That is also why it is considered best practice in the industry to maintain bug bounty programs or other channels for external reports of vulnerability findings—because it is expected that software will always contain vulnerabilities that were not caught during development. The fact that SolarWinds was

³⁶⁸ Graff Report ¶ 188 (citing H. Griffiths Dep. Tr. at 42:17-51:9).

³⁶⁹ See H. Griffiths Dep. Tr. at 42:17-51:9 (“So it’s always possible for anyone ... to find different results and different findings, that’s common across the industry ... [T]hey could be using a completely different product that has, you know, patented or specific rules, scanning that only their product has ... As mentioned, there’s so many of these tools out there.”).

³⁷⁰ See *Google: Vulnerability Statistics*, CVEdetails.com (last visited Nov. 22, 2024), <https://www.cvedetails.com/vendor/1224/Google.html> (reporting vulnerabilities of various types publicly reported for Google products each year); *Microsoft: Vulnerability Statistics*, CVEdetails.com (last visited Nov. 22, 2024), <https://www.cvedetails.com/vendor/26/Microsoft.html> (same for Microsoft); *Adobe: Vulnerability Statistics*, CVEdetails.com (last visited Nov. 22, 2024), <https://www.cvedetails.com/vendor/53/Adobe.html> (same for Adobe).

receiving and responding to penetration tests from customers was good practice, not evidence that it failed to do penetration testing itself.

216. In sum, I do not believe that Mr. Graff has offered any evidence that calls into question the accuracy of the Security Statement's representations about its software development lifecycle and his report therefore does nothing to change my opinions in that regard.

Signed on December 30, 2024, in Andover, New Jersey.



Greg Rattray